

ARITHMETIC OF EISENSTEIN QUOTIENTS

YUAN REN

ABSTRACT. In this paper, we will study the arithmetic of the Eisenstein part of the modular Jacobians. In the first section, we introduce some general preliminaries of the arithmetic theory of modular curves that we will need later. In the second section, we give an example of modular abelian varieties due to Gross and study its properties in some details. In the third section, we define Eisenstein quotients of the modular Jacobians in general and give a criterion of the non-triviality of Heegner points on such Eisenstein quotients. The last two sections return to the concrete examples when the level of the modular Jacobian is a prime or a square of a prime.

CONTENTS

1. Modular curves	1
1.1. Modular curves	1
1.2. Moduli interpretation	2
1.3. Hecke operators	2
2. On the 2-Selmer groups of the Gross curves	3
2.1. CM theory and descent	4
2.2. Gross curves	6
2.3. Computation of the 2-Selmer group	7
2.4. Numerical examples	10
3. Heegner points on Eisenstein quotients	11
3.1. Eisenstein quotients	11
3.2. Eisenstein descent	12
3.3. η -quotient	13
4. Prime level case	13
4.1. Eisenstein quotients	14
4.2. Heegner points on $\widetilde{J^{(q)}}$ for odd q	14
4.3. Heegner points on $\widetilde{J^{(2)}}$	15
5. Level p^2 case	15
5.1. Eisenstein quotients	15
5.2. Structure of $J[m_q]$	17
5.3. Gross curves and the 2-Eisenstein quotient	18
5.4. Heegner point on $\widetilde{J^{(q)}}$ for odd q	18
5.5. Heegner point on Gross curves when $p \equiv 7 \pmod{8}$	20
References	20

1. MODULAR CURVES

1.1. Modular curves. Let $\mathfrak{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ be the upper half plane, $\mathfrak{H} = \mathfrak{H}$ and $Gl_2^+(\mathbb{R}) = \{g \in Gl_2(\mathbb{R}) : \det(g) > 0\}$. There is an action of $Gl_2^+(\mathbb{R})$ on \mathfrak{H} as

$$Gl_2^+(\mathbb{R}) \times \mathfrak{H} \rightarrow \mathfrak{H}, (g, z) \mapsto gz$$

where $gz = \frac{az+b}{cz+d}$ for any $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

A subgroup Γ of $SL_2(\mathbb{Z})$ is called a congruence subgroup if $\Gamma \supseteq \Gamma(N)$ for some positive integer N . Here $\Gamma(N)$ is the subgroup of $SL_2(\mathbb{Z})$ which is congruent to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ modulo N .

For example, for any positive integer N , the group

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

is a congruence subgroup.

In the following, we always assume Γ to be a congruence subgroup.

let $Y_\Gamma = \Gamma \backslash \mathfrak{H}$ be the quotient space, then it is shown in [?] that there is a structure of Reimaa surface on Y_Γ . More over, let $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ acted by $SL_2(\mathbb{Z})$ as the above formula, and define

$$X_\Gamma = \Gamma \backslash \mathfrak{H}^*$$

X_Γ is a compact Riemann surface which is the compactification of Y_Γ . Let $S_\Gamma = \Gamma \backslash \mathbb{P}^1(\mathbb{Q})$ and call it the set of cusps of X_Γ , then it is easy to see S_Γ is a finite subset of X_Γ and $X_\Gamma = Y_\Gamma \cup S_\Gamma$. We shall call X_Γ the modular curve of level Γ .

It is known that a compact Riemann surface is algebraic over \mathbb{C} (GAGA). The important thing here is that these modular curves have algebraic models defined over number fields. Let's explains this for the curves $X_0(N) := \Gamma_0(N) \backslash \mathfrak{H}^*$.

1.2. Moduli interpretation. An elliptic curve E over the complex number field \mathbb{C} is a Riemann surface of genus one. So as a complex manifold, it is of the form \mathbb{C}/L for some lattice L and with the natural group structure, it is an abelian variety of dimension one over \mathbb{C} . Two such abelian varieties $E_i = \mathbb{C}/L_i$ ($i = 1, 2$) are isomorphic if and only if there is a number $\lambda \in \mathbb{C}$ such that $L_2 = \lambda L_1$, and the corresponding isomorphism is just the one induced by multiplication by λ . Hence we have a natural bijection between the upper half plane and the isomorphism classes of elliptic curves over \mathbb{C}

$$SL_2(\mathbb{Z}) \backslash \mathfrak{H} \rightarrow \{E/\mathbb{C}\} / \sim$$

which sends $z \in \mathfrak{H}$ to the class represented by the elliptic curve $E_z = \mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z})$.

More generally, we have the following

Proposition 1.1. *For any positive integer N , here is a natural bijection between $Y_0(N)$ and the isomorphism classes of the pairs of elliptic curves over \mathbb{C} with a cyclic group of order N*

$$Y_0(N) \rightarrow \{E/\mathbb{C}\} / \sim$$

which sends $z \in \mathfrak{H}$ to the class represented by the elliptic curve $(E_z, < \frac{1}{N} >)$.

More over, one can define elliptic curves with level structure algebraically, then the solution of the corresponding moduli problem will gives the desired model over canonically define number field ([10]).

Remark 1.2. In Delinge and Rapapport's paper, they also gives a moduli intercalation of the compact modular curve in terms of generalized elliptic curves with level structure.

1.3. Hecke operators. (modular forms and its relation to differential; Definition of Hecke operator; eigenform and Galois representation of it; modular abelian variety) In this section, we write $X = X_0(N)/\mathbb{Q}$, $J = J_0(N)/\mathbb{Q}$ be its Jacobian and $i : X \rightarrow J$ the canonical morphism mapping ∞ to the zero. Recall that $Y = Y_0(N) = \Gamma_0(N) \backslash \mathfrak{H}$ is an open affine sub-scheme of X which classifies the isomorphism class of pairs $[E, D]$, where E is an elliptic curve and D is a subgroup scheme isomorphic to $\mathbb{Z}/N\mathbb{Z}$.

For any two curves C_1, C_2 over some field F , a correspondence $T : C_1 \rightsquigarrow C_2$ is by definition a triple (C_3, α, β) , where C_3 is another curve and α, β are morphisms from C_3 to C_1 and C_2 respectively. From a correspondence T , one deduce two morphisms on Jacobians: the push forward $T_* : J(C_1) \rightarrow J(C_2)$ defined as $\beta_* \circ \alpha^*$ and the pull back $T^* : J(C_2) \rightarrow J(C_1)$ defined as $\alpha_* \circ \beta^*$.

For any prime ℓ , let $X_0(N, \ell)$ to be the modular curve classifies the isomorphism classes $[E, D, C]$ with E an elliptic curve, D a subgroup scheme isomorphic to $\mathbb{Z}/N\mathbb{Z}$, C a subgroup scheme isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ such that $D \cap C = 0$. Define

$$\alpha_\ell : X_0(N, \ell) \rightarrow X, [E, D, C] \rightarrow [E, D]$$

and

$$\beta_\ell : X_0(N, \ell) \rightarrow X, [E, D, C] \rightarrow [E/C, D + C/C]$$

The Hecke correspondence T_ℓ is defined to be $(X_0(N, \ell), \alpha_\ell, \beta_\ell)$. As mentioned above, we will have two morphisms $T_{\ell,*}$ and T_ℓ^* on J .

Proposition 1.3. *Notations as above, then we have*

$$T_{\ell,*} = T_{\ell}^* = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} + \sum_{k=0}^{\ell-1} \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix}, \ell \nmid N$$

and when $\ell \mid N$, we have

$$T_{\ell,*} = \sum_{k=0}^{\ell-1} \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix}$$

and

$$T_{\ell}^* = \sum_{k=0}^{\ell-1} \begin{pmatrix} \ell & 0 \\ Nk & 1 \end{pmatrix}$$

Proof. First, we assume $\ell \nmid N$. For any $(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) \in X$, we have

$$\alpha^{-1}(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) = (\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} > + < \frac{1}{\ell} >) + \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} > + < \frac{z+k}{\ell} >)$$

so we have

$$T_{\ell,*}(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) = (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z}), < \frac{1}{N} >) + \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \frac{z+k}{\ell} + \mathbb{Z}), < \frac{1}{N} >)$$

Similarly, because we have

$$\beta^{-1}(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) = (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z}), < \frac{1}{N} > + < z >) + \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \frac{z+k}{\ell} + \mathbb{Z}), < \frac{1}{N} > + < \frac{1}{\ell} >)$$

so we also have

$$T_{\ell}^*(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) = (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z}), < \frac{1}{N} >) + \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \frac{z+k}{\ell} + \mathbb{Z}), < \frac{1}{N} >)$$

When $\ell \mid N$, the identity for $T_{\ell,*}$ is similar except we need to omit the term $(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} > + < \frac{1}{\ell} >)$ because $< \frac{1}{N} > \supseteq \frac{1}{\ell}$.

On the other hand, we have

$$\beta^{-1}(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) = \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z}), < \frac{1}{N} + kz >) = \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z}), < \frac{Nkz+1}{N} >)$$

so we have

$$\begin{aligned} \beta^{-1}(\mathbb{C}/(\mathbb{Z} \cdot z + \mathbb{Z}), < \frac{1}{N} >) &= \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z}), < \frac{Nkz+1}{N} >) \\ &= \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \ell z + \mathbb{Z} \cdot Nkz + 1), < \frac{Nkz+1}{N} >) \\ &= \sum_{k=0}^{\ell-1} (\mathbb{C}/(\mathbb{Z} \cdot \frac{\ell z}{Nkz+1} + \mathbb{Z}), < \frac{1}{N} >) \end{aligned}$$

This proves our second claim. □

Definition 1.4. *For any N , we define $\mathbb{T} = \mathbb{Z}[\{T_{\ell,*}\}_{\ell}] \subseteq \text{End}(J)$, and call it the (full) Hecke algebra of level N .*

For simplicity, we will write T_{ℓ} instead of $T_{\ell,*}$ in the following.

2. ON THE 2-SELMER GROUPS OF THE GROSS CURVES

In this section, we will study the 2-Selmer group of some elliptic curves constructed by Gross in [5]. We will show in later sections the relation of these curves with some 2-Eisenstein quotients of level a square of a prime.

2.1. CM theory and descent. Let F be a field, an elliptic curve over F is a smooth curve of genus one over F with an F -rational point O . It is well known that such a curve admits a structure of abelian variety of dimension one such that O is zero element.

Suppose F is a number field, the Mordell-Weil theorem claims that the group of F -rational points $E(F)$ is a finitely generated abelian group, so that $E(F) \simeq \mathbb{Z}^{\oplus r} \oplus E(F)_{\text{tor}}$ with $E(F)_{\text{tor}}$ a finite group, for some non-negative integer r called the rank of E over F . In number theory, we are interested in determining the rank so that solve the Diophantine question. For this, there is the classical descent method.

Recall that from

$$0 \longrightarrow E(F)[n] \longrightarrow E(\bar{F}) \xrightarrow{n} E(\bar{F}) \longrightarrow 0$$

we get the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E()/nE^{(d)}(p) & \xrightarrow{\delta} & H^1(G_F, E[n]) & \longrightarrow & H^1(G_F, E[n]) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod E(F_v)/nE^{(d)}(p)(F_v) & \xrightarrow{\delta_v} & \prod H^1(G_{F_v}, E[n]) & \longrightarrow & \prod H^1(G_{F_v}, E) \longrightarrow 0 \end{array}$$

Definition 2.1. Define the n -Selmer group of E over F to be

$$\text{Sel}_n(E/F) = \ker(H^1(G_F, E[n]) \rightarrow \prod H^1(G_{F_v}, E))$$

and the Tate-Shafarevich group of E over F to be

$$\text{III}(E/F) = \ker(H^1(G_F, E) \rightarrow \prod H^1(G_{F_v}, E))$$

It follows that there is an exact sequence

$$0 \longrightarrow E(F)/nE(F) \xrightarrow{\delta} \text{Sel}_n(E/F) \longrightarrow \text{III}(E/F)[n] \longrightarrow 0$$

The reason to introduce the Selmer groups is that $\text{Sel}_n(E/F)$ is finite and relatively easy to compute, so that one can use them to obtain an upper bound of the rank. In the following, we will focus on the elliptic curves with complex multiplication and analyze the above exact sequence in some details for the so called \mathbb{Q} -curves when $n = 2$.

First we introduce the following notations:

- K = an imaginary quadratic extension over \mathbb{Q} ;
- \mathcal{O} = the integer ring of K ;
- $ELL(\mathcal{O}) = \{\text{elliptic curve over } \mathbb{C} \text{ with CM by } \mathcal{O}\}$ up to C -isomorphism;
- H = the Hilbert class field of K ;
- $ELL_H(\mathcal{O}) = \{\text{elliptic curve over } H \text{ with CM by } \mathcal{O}\}$ up to H -isomorphism;
- $ELL_H^\circ(\mathcal{O}) = \{\text{elliptic curve over } H \text{ with CM by } \mathcal{O}\}$ up to H -isogeny;

Recall the following basic facts from CM theory, c.f. [3]:

Proposition 2.2. For any E in $ELL_H(\mathcal{O})$, we have an associated continuous homomorphism $\chi_E : \mathbb{A}_H^\times \rightarrow K^\times$ such that

- (i) $\chi|_{H^\times} = \mathbf{N}_K^H$, where \mathbf{N}_K^H is the norm map from H to K ;
- (ii) E has good reduction at $\beta \in \text{Spec } \mathcal{O}_H$ if and only if χ_E is unramified at β . If E has good reduction at $\beta \in \text{Spec } \mathcal{O}_H$, then $\chi_E(\pi_\beta)$ is the unique lifting of the $\mathbf{N}(\beta)$ -th Frobenius of $\tilde{E} \pmod{\beta}$;
- (iii) for any rational prime ℓ , we have $\rho_\ell = \chi_E \cdot (\mathbf{N}_{K_\ell}^{H_\ell})^{-1}$, where $\rho_\ell : G_H \rightarrow T_\ell$ is the ℓ -adic Galois representation, $H_\ell = \prod_{w|\ell} H_w$ and $\mathbf{N}_{K_\ell}^{H_\ell}$ is the norm.

We now review the H -isomorphic and H -isogenous classifications of elliptic curves with CM by \mathcal{O} .

Theorem 2.3. Let $J = \{j(E) \mid E \in ELL(\mathcal{O})\}$, and Σ be the set of continuous homomorphism $\chi : \mathbb{A}_H^\times \rightarrow K^\times$ such that $\chi|_{H^\times} = \mathbf{N}_K^H$, where \mathbf{N}_K^H is the norm map from H to K , then

(i) There is a bijection

$$ELL_H(\mathcal{O}) \rightarrow J \times \Sigma, \quad E/H \mapsto (j(E), \chi_E);$$

(ii) There is a bijection

$$ELL_H^\circ(\mathcal{O}) \rightarrow \Sigma, \quad E/H \mapsto \chi_E.$$

Lemma 2.4. For any $E \in \mathcal{ELL}_{\mathcal{H}}(\mathcal{O})$ and $\psi : G_H \rightarrow \mathcal{O}^\times$ a continuous homomorphism, let E^ψ denote twist of E by ψ (note that $\mathcal{O}^\times = \text{Aut}(E)$), then $\chi_{E^\psi} = \psi \cdot \chi_E$.

Proof. Recall E^ψ is the ψ -twist of E means there is a \bar{H} -isomorphism $\phi : E \rightarrow E^\psi$ such that for any $g \in G_H$, $\psi(g) = \phi^{-1} \circ \phi^g$. Fix such a ϕ .

Let w be a place where χ_{E^ψ} , $\psi \cdot \chi_E$ and ψ are all unramified. Then from $\psi^{\sigma(w)} = \phi^{-1} \circ \phi^{\sigma(w)}$, we have $\psi^{\sigma(w)} = \phi^{-1} \circ \phi^{q_w} \pmod{w}$. So that as morphism, we have

$$\psi^{\sigma(w)} \circ [\chi_E(w)] = \phi^{-1} \circ [\chi_{E^\psi}(w)] \circ \phi \pmod{w},$$

which implies that $\psi^{\sigma(w)} \cdot \chi_E(w) = \chi_{E^\psi}(w)$ by acting on the invariant differential.

As both $\chi_{E^\psi} = \psi \cdot \chi_E$ when restrict to H^\times , the approximation theorem implies that they are the same on an open dense subset of \mathbb{A}_H^\times and the assertion follows. \square

Lemma 2.5. *Let $E_1, E_2 \in \mathcal{ELL}_{\mathcal{H}}(\mathcal{O})$, $\phi : E_1 \rightarrow E_2$ an \bar{H} -isogeny. Define*

$$\psi : G_H \rightarrow \mathcal{O}^\times, g \mapsto \frac{\hat{\phi} \circ \phi^g}{\deg \phi} \in H^1(G_H, \mathcal{O}^\times).$$

Then $\chi_{E_2} = \psi \cdot \chi_{E_1}$.

Proof. As in the proof of Lemma 2.4, for all but finitely many w , because $\hat{\phi} \circ \phi^{\sigma(w)} = \deg \phi \cdot \psi(w)$, $\hat{\phi} \circ \phi^{q_w} = \deg \phi \cdot \psi(w) \pmod{w}$, which means $\hat{\phi} \circ [\chi_{E_2}(w)] \circ \phi^{q_w} = \deg \phi \cdot \psi(w) \circ \chi_{E_1}(w) \pmod{w}$.

Because $\hat{\phi} \circ \phi = \deg \phi$, acting on the invariant differential gives that $\deg \phi \cdot \chi_{E_2}(w) = \deg \phi \cdot \psi(w) \cdot \chi_{E_1}(w)$, then we have $\chi_{E_2} = \psi \cdot \chi_{E_1}$. \square

Proof of Theorem 2.3. (c.f. [3]) (i) $j(E_1) = j(E_2)$ implies that there is a \bar{H} -isomorphism $\phi : E_1 \rightarrow E_2$, so if define $\psi : G_H \rightarrow \mathcal{O}^\times, g \mapsto \phi^{-1} \circ \phi^g$ as in Lemma 2.4, then $E_2 = E_1^\psi$, and $\chi_{E_2} = \psi \cdot \chi_{E_1}$. But then the assumption implies that $\psi = 1$, i.e. ϕ is defined over H , so $E_1 = E_2$ in $\mathcal{ELL}_{\mathcal{H}}(\mathcal{O})$.

(ii) For any E_1, E_2 , choose a $\phi \in \text{Hom}(E_1, E_2)$ which is a \bar{H} -isogeny, and define ψ as in Lemma 2.5, then $\chi_{E_2} = \psi \cdot \chi_{E_1}$. Because $\chi_{E_1} = \chi_{E_2}$, we have $\psi = 1$, which means ϕ is defined over H . \square

Recall the definition of \mathbb{Q} -curves:

Definition 2.6. *$E \in \text{ELL}_H(\mathcal{O})$ is called a \mathbb{Q} -curve, if for any $\sigma \in \text{Gal}(H/\mathbb{Q})$, we have $E^\sigma = E$ in $\mathcal{ELL}_{\mathcal{H}}^{\circ}(\mathcal{O})$.*

We will now describe the descent method used in [3].

Lemma 2.7. *Let $E \in \mathcal{ELL}_{\mathcal{H}}(\mathcal{O})$ be a \mathbb{Q} -curve. Then for any $\sigma \in G$,*

$$\text{Hom}(E^\sigma, E)/2 \text{Hom}(E^\sigma, E) \cong \mathcal{O}/2\mathcal{O}.$$

Proof. Assume $E[2]$ is generated by P over $\mathcal{O}/2\mathcal{O}$, so $E^\sigma[2]$ is generated by P^σ . For any $\phi \in \text{Hom}(E^\sigma, E)$, let $[a_\phi] \in \mathcal{O}/2\mathcal{O}$ such that $\phi(P^\sigma) = a_\phi \cdot P$, this gives a homomorphism $\text{Hom}(E^\sigma, E)/2\text{Hom}(E^\sigma, E) \rightarrow \mathcal{O}/2\mathcal{O}$, which is obviously injective. On the other hand, the density theorem implies that this homomorphism is surjective. \square

Recall that from

$$0 \longrightarrow E(H)[2] \longrightarrow E(\bar{H}) \xrightarrow{2} E(\bar{H}) \longrightarrow 0$$

we get the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(H)/2E^{(d)}(p) & \xrightarrow{\delta} & H^1(G_H, E[2]) & \longrightarrow & H^1(G_H, E[2]) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod E(H_v)/2E^{(d)}(p)(H_v) & \xrightarrow{\delta_v} & \prod H^1(G_{H_v}, E[2]) & \longrightarrow & \prod H^1(G_{H_v}, E[2]) \longrightarrow 0 \end{array}$$

For any \mathbb{Q} -curves E , we can give $E(H)/2E(H)$, $\text{Sel}_2(E/H)$ and $\text{III}(E/H)[2]$ a structure of $\text{Gal}(H/Q)$ -module by using Lemma 2.7 as following

- For any $\sigma \in \text{Gal}(H/K)$ and $x \in E(H)/2E(H)$, define

$$\sigma(x) = \phi(x^\sigma)$$

where $\phi \in \text{Hom}(E^\sigma, E)$ is chosen so that ϕ maps to 1 under the isomorphism in Lemma 2.7

- For any $\sigma \in \text{Gal}(H/K)$ and $x \in \text{Sel}_2(E/H)$, define

$$\sigma(x) = \phi(x^\sigma)$$

where $\phi \in \text{Hom}(E^\sigma, E)$ is chosen so that ϕ maps to 1 under the isomorphism in Lemma 2.7

- For any $\sigma \in \text{Gal}(H/K)$ and $x \in \text{III}(E/H)[2]$, define

$$\sigma(x) = \phi(x^\sigma)$$

where $\phi \in \text{Hom}(E^\sigma, E)$ is chosen so that ϕ maps to 1 under the isomorphism in Lemma 2.7.

It is easy to verify the above actions are independent of the choose of ϕ .

Proposition 2.8. *The exact sequence*

$$0 \longrightarrow E(H)/2E(H) \xrightarrow{\delta} \text{Sel}_2(E/H) \longrightarrow \text{III}(E/H)[2] \longrightarrow 0$$

is an exact sequence of $\text{Gal}(H/Q)$ modules.

Proof. It is enough to show δ is a homomorphism of $\text{Gal}(H/Q)$ -modules.

For any $P \in E(H)/2E(H)$, assume $[2]Q = P$, then $\delta(P)(g) = Q^g - Q$, for any $g \in G_H$. Choose $\phi \in \text{Hom}(E^\sigma, E)$ such that $\phi \equiv 1(2)$, then we have by definition $\sigma(P) = \phi(P^\sigma)$, so

$$\begin{aligned} [\delta(\sigma(P))](g) &= [\delta(\phi(P^\sigma))](g) \\ &= g(\phi(Q^\sigma) - \phi(Q^\sigma)) = \phi(g(Q^\sigma) - \phi(Q^\sigma)) \\ &= \phi \circ \sigma[\sigma^{-1}g\sigma(Q) - Q] = \sigma[\delta(P)(g)], \end{aligned}$$

the proposition then follows. \square

2.2. Gross curves. Let p be a rational prime with $p > 3$ and $p \equiv 3 \pmod{4}$. Let $K = \mathbb{Q}(\sqrt{-p})$, \mathcal{O} the integer ring of K , $H = H_K$ be the Hilbert class field of K . For any ideal $a \subseteq \mathcal{O}$, let $K(a)$ be the ray class field modulo a .

Consider the continuous homomorphism $\phi_0 : K^\times (\prod_v \mathcal{O}_v^\times) \rightarrow K^\times (\mathcal{O}_\infty^\times := C^\times)$ satisfying

- (1) $\phi_0|_{K^\times} = \text{id}_{K^\times}$
- (2)

$$\begin{array}{ccc} \prod_v \mathcal{O}_v^\times & \longrightarrow & \{\pm 1\} \\ \downarrow & & \uparrow \delta \\ \prod_{v|(\sqrt{-p})} \mathcal{O}_v^\times & \longrightarrow & (\mathcal{O}/(\sqrt{-p}))^\times \end{array}$$

Here δ maps $x = a + b\frac{1+\sqrt{-p}}{2}$ ($a, b \in \mathbb{Z}$) to $(\frac{x \pmod{\sqrt{-p}}}{p}) = (\frac{a+\frac{b}{2}}{p})$, where $(\frac{\cdot}{p})$ is the Jacobi symbol. Note that $p \equiv 3 \pmod{4}$ ensures this ϕ_0 is well defined.

From

$$0 \longrightarrow K^\times (\prod_v \mathcal{O}_v^\times) \longrightarrow A_{K^\times} \longrightarrow Cl(K) \longrightarrow 0$$

we get

$$0 \longrightarrow \text{Hom}(Cl(K), \bar{K}^\times) \longrightarrow \text{Hom}(A_{K^\times}, \bar{K}^\times) \longrightarrow \text{Hom}(K^\times (\prod_v \mathcal{O}_v^\times), \bar{K}^\times) \longrightarrow 0$$

because $\text{Ext}^1(Cl(K), \bar{K}^\times) = 0$ as \bar{K}^\times is divisible hence injective. From this, we have

Theorem 2.9. *There is a continuous homomorphism $\phi : \mathbb{A}_{K^\times} \rightarrow \bar{K}^\times$ such that $\phi|_{K^\times (\prod_v \mathcal{O}_v^\times)} = \phi_0$; in particular this character is of conductor $(\sqrt{-p})$. This character is unique up to $\widehat{Cl(K)}$.*

Let $\chi : \mathbb{A}_H^\times \rightarrow K^\times$ be defined as $\chi = \phi \circ N_K^H$ where N_K^H is the norm map.

By the CM theory, there is a unique isogeny class of elliptic curves over H with CM \mathcal{O} and the associated character χ . We will call any elliptic curves in this isogeny class a Gross curve of level p .

Here are the basic properties of the Gross curves ([5]):

Theorem 2.10. *Let E be a Gross curve and $F = \mathbb{Q}(j(E))$, then we have*

- (1) $E(F)_{\text{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ or 0, according to whether $(\frac{2}{p}) = 1$ or -1 ;
- (2) The ϵ -factor of $L(E/F, s)$ equals to $(\frac{2}{p})$.

2.3. Computation of the 2-Selmer group. In this subsection, we assume $p \equiv 7 \pmod{8}$. We will use the method in section 2.1 to compute the rank of some quadratic twists of the Gross curve. Note that in K , we have $(2) = \omega\bar{\omega}$ with $\omega = (\frac{1+\pi}{2}, 2)$ and $\mathcal{O}^\times = \{\pm 1\}$.

In [3], Gross established the following results.

Proposition 2.11. *Notations as above, then for any Gross curve E , we have*

$$E^{(d)}(H)/2E^{(d)}(H) \cong \mathcal{O}/2\mathcal{O} \bigoplus (\mathcal{O}/2\mathcal{O}[\text{Gal}(H/K)])^{n(d)}$$

with some integer $n(d)$ (so that $n(d) \cdot h_K = \text{rank}_{\mathcal{O}} E^{(d)}(H)$).

In particular, we have $n(d) + 1 \leq \text{rank}_{\mathcal{O}/2\mathcal{O}}(\text{Sel}_2(E^{(d)}/H))^{\text{Gal}(H/K)}$.

Lemma 2.12. *For any two Gross curves E_1, E_2 , we have $\text{Sel}_2(E_1/H) \cong \text{Sel}_2(E_2/H)$ as $\text{Gal}(H/K)$ -modules.*

Proof. As $E_i[2] \subseteq E_i(H)$, we have $H^1(G_H, E_i[2]) \cong \text{Hom}(G_H, E_i[2])$.

The density theorem implies there is an \bar{H} -isogeny $\phi : E_1 \rightarrow E_2$ such that $\deg(\phi)$ is odd. But E_1 and E_2 are H -isogenous, so by Lemma 2, we have ϕ is an H -isogeny.

This ϕ induces a group isomorphism (also denoted by ϕ) $\phi : \text{Hom}(G_H, E_1[2]) \rightarrow \text{Hom}(G_H, E_2[2])$, sending $\psi \in \text{Hom}(G_H, E_1[2])$ to $\phi \circ \psi$. We know from Proposition 2.11 that $E_i[2]$ are trivial $\text{Gal}(H/K)$ -modules. So for any $\psi \in \text{Hom}(G_H, E_1[2])$, $g \in G_H$ and $\sigma \in \text{Gal}(H/K)$, we have $(\phi \circ \psi)^\sigma(g) = \sigma(\phi \circ \psi(\sigma^{-1}g\sigma)) = \phi \circ \psi(\sigma^{-1}g\sigma) = \phi(\sigma(\psi(\sigma^{-1}g\sigma))) = \phi(\psi^\sigma(g)) = \phi \circ \psi^\sigma(g)$, i.e. ψ is a homomorphism of $\text{Gal}(H/K)$ -modules. And this gives the desired homomorphism between $\text{Sel}_2(E_1/H)$ and $\text{Sel}_2(E_2/H)$. \square

In the following, we write $S^{(d)}$ for $(\text{Sel}_2(E^{(d)}/H))^{\text{Gal}(H/K)}$ (for any $E \in [C]$). By Lemma 2.12, we only need to compute $S^{(d)}$ for any fixed $E \in [C]$. But we have the following

Lemma 2.13. *There is a unique Gross curve $E(p)$ such that $\Delta(E(p)/F) = (-p^3)$, where $F = \mathbb{Q}(j(E))$.*

Proof. C.f. [3], Theorem 12.2.1. \square

We will do the computation for this $E(p)$.

Recall that from

$$0 \longrightarrow E^{(d)}(p)(H)[2] \longrightarrow E^{(d)}(p)(\bar{H}) \xrightarrow{2} E^{(d)}(p)(\bar{H}) \longrightarrow 0$$

we get the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{E^{(d)}(p)(H)}{2E^{(d)}(p)} & \xrightarrow{\delta} & H^1(G_H, E^{(d)}(p)[2]) & \longrightarrow & H^1(G_H, E^{(d)}(p))[2] \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod \frac{E^{(d)}(p)(H_v)}{2E^{(d)}(p)(H_v)} & \xrightarrow{\delta_v} & \prod H^1(G_{H_v}, E^{(d)}(p)[2]) & \longrightarrow & \prod H^1(G_{H_v}, E^{(d)}(p))[2] \longrightarrow 0 \end{array}$$

Lemma 2.14. *There is a basis of $E^{(d)}(p)[2]$, such that*

$$\text{im}(\delta_v) = \{(x, y) \in H_v^\times / H_v^{\times 2} : x \in 1 + \omega^2 \mathcal{O}_v^\times, y \in 1 + \omega \mathcal{O}_v^\times\}$$

for all place v of H over ω , and

$$\text{im}(\delta_w) = \{(x, y) \in H_w^\times / H_w^{\times 2} : x \in 1 + \bar{\omega} \mathcal{O}_w^\times, y \in 1 + \bar{\omega}^2 \mathcal{O}_w^\times\}$$

for all place w of H over $\bar{\omega}$.

Proof. First, we show $E(p)$ has ordinary reduction at every place v of H over ω and the same for places over $\bar{\omega}$. Suppose $N(\wp_v) = (\wp_v)^{f(v/\omega)} = (f_\omega)$, then $\chi_p(\pi_v) = \pm f_\omega$. We need to show that $a_v = \pm(f_\omega + \bar{f}_\omega)$ is odd. Assume $f_\omega = x + y \cdot \frac{1+\pi}{2}$ with $a, b \in \mathbb{Z}$, then $a_v = \pm(y + 2a)$. As $Nf_\omega = f_\omega \cdot \bar{f}_\omega = (N\wp_v)^{f(v/\omega)} = 2^{f(v/\omega)}$, we have $x^2 + xy + y^2 \cdot \frac{1+\pi}{4} = 2^{f(v/\omega)}$ which is even. If $2 \mid y$, then $2 \nmid x$ because $2 \nmid f_\omega$, then $x^2 + xy + y^2 \cdot \frac{1+\pi}{4}$ is odd which is a contradiction, so $2 \nmid y$ and a_v is odd. Now it follows that $E(p)^{(d)}$ has good ordinary reduction because its character differs from χ_p by a quadratic character unramified over 2.

From [2], Lemma 3.5, there is a unique two torsion point P_1 such that $P_1 \equiv \mathcal{O} \pmod{\omega}$. Because $\Delta(E(p)/F) = (-p^3)$ is odd, P_1 can not belongs to $E(p)(F)$ for otherwise P_1 will be 2-integral which contradicts to $P_1 \equiv \mathcal{O} \pmod{\omega}$. Let $P_2 = \bar{P}_1$, then P_2 is the unique two torsion such that $P_2 \equiv \mathcal{O} \pmod{\bar{\omega}}$. The assertion follows from [2], Proposition 3.6 by taking P_1, P_2 as the basis. \square

To state our results, we introduce the following notations.

Let $d = \prod_{i=1}^n (-q_i) \cdot \prod_{j=1}^m (q'_j) \cdot \prod_{k=1}^l (Q_k^*)$ be an integer congruent to 1 modulo 4, where q_i, q'_j are primes split in K and Q_k are primes inertia in K with $q_i \equiv 3 \pmod{4}$ and $q'_j \equiv 1 \pmod{4}$.

Let $h = h_K$, then $q_i^h = f_i \cdot \bar{f}_i$ and $q'_j{}^h = g_j \cdot \bar{g}_j$ with $f_i, g_j \in \mathcal{O}_K$.

Lemma 2.15. *Notation as above, we may assume $f_i = a_i + b_i \frac{1+\pi}{2}$ with $a_i \equiv 1 \pmod{4}$ and $v_2(b_i) = 1$; $g_j = a'_j + b'_j \frac{1+\pi}{2}$ with $a'_j \equiv 1 \pmod{4}$ and $v_2(b'_j) \geq 2$.*

Proof. Write $f_i = a_i + b_i \frac{1+\pi}{2}$, then $a_i^2 + a_i b_i + b_i^2 \frac{1+\pi}{4} = q_i^h$ is odd, so it is easy to see that $2 \nmid a_i$ but $2 \mid b_i$, and hence we can multiply it by ± 1 so that $a_i \equiv 1 \pmod{4}$.

Now we have $f_i - 1 \equiv 0 \pmod{2\omega}$ and $\bar{f}_i - 1 \equiv 0 \pmod{2\bar{\omega}}$, so $(f_i - 1)(\bar{f}_i - 1) \equiv 0 \pmod{4}$. On the other hand, $f_i \cdot \bar{f}_i - 1 = q_i^h - 1 \equiv 2 \pmod{4}$ because h is odd by the genus theory, so $(f_i - 1) + (\bar{f}_i - 1) \equiv 2 \pmod{4}$, i.e. $b_i + 2(a_i - 1) \equiv 2 \pmod{4}$, then we have $b_i \equiv 2 \pmod{4}$.

The proof for the second assertion is similar. \square

Lemma 2.16. *Let $d \equiv 1 \pmod{4}$ be an integer and notations as above, then we have*

- (i) $E^{(d)}(p)$ has good reduction at all the places not dividing pd ;
- (ii) There is a basis of $E^{(d)}(p)[2]$, such that

$$S^{(d)} \subseteq H_d := \{(\alpha, \beta) \in (K^\times / K^{\times 2})^2 \mid \alpha = (-\pi)^a \prod_{i=1}^n [f_i^{s_i} \cdot (-\bar{f}_i^{t_i})] \cdot \prod_{j=1}^m [g_j^{r_j} \cdot \bar{g}_j^{u_j}] \cdot \prod_{k=1}^l [(Q_k^*)^{v_k}],$$

$$\beta = (\pi)^{a'} \prod_{i=1}^n [(-f_i^{s'_i}) \cdot \bar{f}_i^{t'_i}] \cdot \prod_{j=1}^m [g_j^{r'_j} \cdot \bar{g}_j^{u'_j}] \cdot \prod_{k=1}^l [(Q_k^*)^{v'_k}]\}$$

where $a, \dots, v'_k = 0$ or 1 ;

- (iii) For any $v \nmid 2$, we have $\#im(\delta_v) = 4$.

Proof. (i) This is because $E(p)$ only has bad reduction at the places over p and d is congruent to 1 mod 4;

(ii) Note that by the genus theory, the order of $\text{Gal}(H/K)$ is odd, so both $H^1(\text{Gal}(H/K), E[2])$ and $H^1(\text{Gal}(H/K), E[2])$ are zero. Then by the Serre-Hoschild exact sequence, we have $H^1(G_K, E[2]) \cong H^1(G_H, E[2])^{\text{Gal}(H/K)}$ and so $S^{(d)} \subseteq H^1(G_K, E[2])$.

If $(\alpha, \beta) \in (K^\times / K^{\times 2})^2$ belongs to $S^{(d)}$, then by Lemma 2.14 and (i) above, we have $\alpha, \beta \in \mathcal{O}_{H_v}^\times$ modulo $(H_v^\times)^2$ (for any $v \nmid pd$). But H is unramified over K , so $\alpha, \beta \in \mathcal{O}_{K_w}^\times$ modulo $(K_w^\times)^2$ (for any $w \nmid pd$). Also because h is odd, we find $\alpha = (\alpha)^h = \pm(\pi) \prod_{i=1}^n [f_i^{s_i} \cdot (\bar{f}_i^{t_i})] \cdot \prod_{j=1}^m [g_j^{r_j} \cdot \bar{g}_j^{u_j}] \cdot \prod_{k=1}^l [(Q_k^*)^{v_k}]$ with $a_i, \dots, v_k = 0, 1$ and similarly for β .

By Lemma 2.14, we can choose a basis of $E(p)[2]$ such that $\alpha \equiv 1 \pmod{\omega^2}$ and $\beta \equiv 1 \pmod{\bar{\omega}^2}$, so we get the result;

(iii) Suppose $v \nmid 2$. By the theory of formal groups, there is $M \subseteq E^{(d)}(p)(H_v)$ such that $M \cong \mathcal{O}_v$ and $E^{(d)}(p)(H_v)/M$ is finite. Consider

Apply snake lemma, we get $|E^{(d)}(p)(H_v)/2A(H_v)| \cdot |\mathcal{O}_v[2]| = |E^{(d)}(p)(H_v)[2]| \cdot |\mathcal{O}_v/2\mathcal{O}_v|$. But as $v \nmid 2$, then we have $|\mathcal{O}_v[2]| = |\mathcal{O}_v/2\mathcal{O}_v| = 1$ and the result follows;

- (iv) Just by the definition of the Selmer group. \square

From Lemma 2.16 we know that to compute $S^{(d)}$, it is necessary to know the image of $E^{(d)}(p)[2]$ under δ . For this, we have the following

Lemma 2.17. *For any $d \in \mathbb{Z}$, there is a basis of $E^{(d)}(p)[2]$ such that*

$$\delta(E^{(d)}(p)[2]) = \{(1, 1), (-\pi d, 1), (1, \pi d), (-\pi d, \pi d)\}.$$

And we have

$$im(\delta_v) = \delta_v(E^{(d)}(p)[2])$$

for any $v \mid pd$.

Proof. For the first assertion, it is enough to verify this for the case $d = 1$. Fix the basis as in Lemma 2.14.

Take a Weierstrass equation over H of $E(p) : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $\Delta(E(p)) = -p^3$. Since $E(p)$ has potentially good reduction everywhere, we can find some finite extension of H such that $E(p)$ has good reduction at π . Then a change of coordinates of the form

$$\begin{cases} x = \pi X + r \\ y = \pi^{\frac{3}{2}} Y + s\pi X + t \end{cases}$$

gives a Weierstrass equation $\mathcal{E}(p) : f(X, Y) = 0$ with good reduction at π . Notice that $P_i = (e_i, 0)$'s are the 2-torsion points, we have

$$v_\pi(X(P_i) - X(P_j)) \geq 0, \forall i \neq j,$$

and then $v_\pi(e_i - e_j) \geq 1$. But $\Delta(E(p)) = -p^3$ implies $2 \sum_{i < j} v_\pi(e_i - e_j) = 6$, hence we have $v_\pi(e_i - e_j) = 1$.

By [?], Proposition 14, we have

$$\begin{aligned} \delta(P_0) &= (x_0, y_0) = (1, 1), \\ \delta(P_1) &= (x_1, y_1) = \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2\right), \\ \delta(P_2) &= (x_2, y_2) = \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right), \\ \delta(P_3) &= (x_3, y_3) = (e_3 - e_1, e_3 - e_2). \end{aligned}$$

Since Lemma 2.16 implies that $x_i, y_i \equiv (-1)^a \pi^b$ with $a, b = 0$ or 1 , by combining the above results and Lemma 2.14, we have

$$\begin{aligned} \delta(P_0) &= (x_0, y_0) = (1, 1), \\ \delta(P_1) &= (x_1, y_1) = (1, \pi), \\ \delta(P_2) &= (x_2, y_2) = (-\pi, 1), \\ \delta(P_3) &= (x_3, y_3) = (-\pi, \pi). \end{aligned}$$

For the second assertion, we note that the four elements

$$(1, 1), (-\pi d, 1), (1, \pi d), (-\pi d, \pi d)$$

are distinct in K_v^\times for any $v \mid pd$, so the result follows from Lemma 2.16, (iii). \square

Now we can prove our main theorem which gives a complete description of the elements in $S^{(d)}$ for $d \equiv 1 \pmod{4}$.

Theorem 2.18. $(\alpha, \beta) \in S^{(d)}$ is equivalent to $(\alpha, \beta) \in H_d$ and there is

$$(x_{i(v)}, y_{i(v)}) \in \{(1, 1), (-\pi d, 1), (1, \pi d), (-\pi d, \pi d)\}$$

such that $\alpha x_{i(v)} \in K_v^{\times 2}$ and $\beta y_{i(v)} \in K_v^{\times 2}$ for any place $v \mid pd$ of K .

Proof. This follows from the definition of Selmer group, combining with Lemma 2.16 and Lemma 2.17. \square

In practice, one can always compute $S^{(d)}$ by Theorem 2.18. In the following, we give a graphical description of it, which seems more convenient to use.

Definition 2.19. Let $d \equiv 1 \pmod{4}$ and f_i, g_j, Q_k as above.

Define a (oriented) graph G_d as following:

vertex of $G_d = \{-\pi, f_i, -\bar{f}_i, g_j, \bar{g}_j, Q_k^*\}_{1 \leq i \leq n, 1 \leq j \leq m, 1 \leq k \leq l}$

arrows of G_d : there exist an arrow from x to y if and only if $(\frac{x}{y}) = -1$ (here the symbol $(\frac{x}{y})$ is the quadratic residue symbol in K)

Theorem 2.20. For every $d \equiv 1 \pmod{4}$, we have

$$\text{rank}_{\mathcal{O}/2\mathcal{O}}(S^{(d)}) = 1 + 2t$$

where t is the number of even partitions of G_d .

In particular, $S^{(d)}$ is minimal if and only if G_d is an odd graph.

Proof. Define graph G'_d with vertex $\{\pi, -f_i, \bar{f}_i, g_j, \bar{g}_j, Q_k^*\}_{1 \leq i \leq n, 1 \leq j \leq m, 1 \leq k \leq l}$, and there is an arrow from x to y if and only if $(\frac{x}{y}) = -1$.

Given $(\alpha, \beta) \in H_d$, we have a partition $V_\alpha \cup V_{n\alpha}$ of G_d with $V_\alpha = \{x : x \mid \alpha\}$, and similarly a partition $V_\beta \cup V_{n\beta}$ of G'_d . Now $(\alpha, \beta) \in S^{(d)}$ means that $(\frac{\alpha}{x}) = 1$ for any $x \nmid \alpha$ and $(\frac{-\pi d/\alpha}{x}) = 1$ for any $x \mid \alpha$, and the same for β which is equivalent to say that $V_\alpha \cup V_{n\alpha}$ and $V_\beta \cup V_{n\beta}$ are even partitions. Note that α and $-\pi d/\alpha$ correspond to the same partition and the same for β and $\pi d/\beta$, we will obtain the assertion if we can show that if we can show the map $\phi : G \rightarrow G'_d, -\pi \mapsto \pi, f_i \mapsto \bar{f}_i, -\bar{f}_i \mapsto -f_i, g_j \mapsto \bar{g}_j, \bar{g}_j \mapsto g_j, Q_k^* \mapsto Q_k^*$ is an isomorphism, i.e. there is an arrow from x to y if and only if there is an arrow from $\phi(x)$ to $\phi(y)$, which is obvious. \square

2.4. Numerical examples.

Lemma 2.21. (i) If Q is a prime such that $(\frac{-p}{Q}) = -1$, then we have $\pm\pi \in (K_Q^\times)^2$ if and only if Q is congruent to 3 modulo 4;

(ii) If Q is a prime such that $(\frac{-p}{Q}) = -1$, then we always have $-1 \in (K_Q^\times)^2$;

(iii) If Q_1 and Q_2 are primes such that $(\frac{-p}{Q_i}) = -1$ ($i = 1, 2$), then we always have $Q_1^* \in (K_{Q_2}^\times)^2$.

Proof. (i) If Q is congruent to 3 modulo 4. By Hensel lemma, it is enough to solve $(a + b\pi)^2 \equiv \pm\pi \pmod{Q}$. This is equivalent to $a^2 - pb^2 \equiv 0 \pmod{Q}$ and $2ab \equiv \pm 1 \pmod{Q}$. So we only need to show $a^4 \equiv \frac{p}{4} \pmod{Q}$ has solution in \mathbb{Z} . But as Q is congruent to 3 modulo 4, we have $(\frac{p}{Q}) = -(\frac{-p}{Q}) = 1$, so there is $x \in \mathbb{Z}$ such that $x^2 \equiv \frac{p}{4} \pmod{Q}$. As one of x and $-x$ is also a square modulo Q , we can then get the solution of $a^4 \equiv \frac{p}{4} \pmod{Q}$.

If Q is congruent to 1 modulo 4, then $(\frac{p}{Q}) = (\frac{-p}{Q}) = -1$, so the equation doesn't have any solutions.

(ii) This is well known if Q is congruent to 1 modulo 4. But (1) above implies this is also true for Q congruent to 3 modulo 4.

(iii) By Hensel lemma, it is enough to solve $(a + b\pi)^2 \equiv Q_1^* \pmod{Q_2}$. This is equivalent to $a^2 - pb^2 \equiv Q_1^* \pmod{Q_2}$ and $2ab \equiv 0 \pmod{Q_2}$. If $(\frac{Q_1^*}{Q_2}) = 1$, then we can get a solution by setting $b \equiv 0$. If $(\frac{Q_1^*}{Q_2}) = -1$, then set $a \equiv 0$ to solve $b^2 \equiv -pQ_1^* \pmod{Q_2}$, which has solution as $(\frac{-pQ_1^*}{Q_2}) = 1$. \square

Theorem 2.22. Let $d = \prod_{i=1}^n Q_i^*$ be a square-free rational integer, where Q_i are odd rational primes such that $(\frac{-p}{Q_i}) = -1$, then

$$E^{(d)}(p)(H) = E^{(d)}(p)[2] \text{ and } (\text{III}(E^{(d)}(p)/H)[2])^{\text{Gal}(H/K)} = 1$$

if and only if $Q_i \equiv 1 \pmod{4}$ for any $i = 1, \dots, n$.

Moreover, we have $\text{rank}_{\mathcal{O}/2\mathcal{O}} S^{(d)} \geq 1 + k$, where k is the number of those Q_i which is congruent to 3 modulo 4.

Proof. If all the Q_i are congruent to 1 modulo 4, we want to show that $(\alpha, \beta) \in S^{(d)}$ implies $(\alpha, \beta) \in \text{im}(E^{(d)}(p)[2])$.

Suppose there is some $(\alpha, \beta) \in S^{(d)}$ not in $\text{im}(E^{(d)}(p)[2])$. then either $\alpha \neq 1, -\pi$ or $\beta \neq 1, \pi$.

If $\alpha \neq 1, -\pi$, multiplying suitable element in $\beta \neq 1, \pi$, we may assume $\pi \mid \alpha$. Then by Lemma 9, we have α is not in $K_{Q_i}^{\times 2}$ for any $Q_i \nmid \alpha$. So we must have $\alpha = 1$ or $-\pi$.

If $\beta \neq 1, \pi$, multiplying suitable element in $\beta \neq 1, \pi$, we may assume $\pi \mid \beta$. Then by Lemma 9, we have β is not in $K_{Q_i}^{\times 2}$ for any $Q_i \nmid \beta$. So we must have $\beta = 1$ or π .

If there is some $Q_i \equiv 1 \pmod{4}$, we claim that $(1, Q_i^*) \in S^{(d)}$. At Q_j for $j \neq i$, we have $Q_i^* \in (K_{Q_j}^\times)^2$; at π , as $\frac{Q_i^*}{p} = \frac{p}{Q_i} = 1$, we also have $(1, Q_i^*) \in \text{im}(\delta_\pi)$; at Q_i , multiply it by $(1, \pi d)$ to get $(1, \pi \prod_{j \neq i} Q_j^*)$ with $\pi \prod_{j \neq i} Q_j^* \in K_{Q_i}^{\times 2}$ by Lemma 2.21. Now the claim follows from Lemma 2.16, (iv). This complete the first assertion of Theorem 2.22.

By the above, we see that we always have $(1, Q_i^*) \in S^{(d)}$ for $Q_i \equiv 3 \pmod{4}$. Since these elements are linearly independent in S^d , we complete the proof of Theorem 2.22. \square

Corollary 2.23. Let d be as in Theorem 2.22 with $d > 0$ and $p > 4d^2 \lg |d|$, then the BSD conjecture is true for $E^{(d)}(p)$ and $\text{III}(E^{(d)}(p)/H)[2] = \text{Sel}_2(E^{(d)}(p)/H)$. In particular, we can construct arbitrarily large Shafarevich-Tate group by choosing p large enough and d contains enough Q which is congruent to 3 modulo 4.

Proof. Under the assumptions on d , we have $L(E^{(d)}(p)/H, 1) \neq 0$ by the main theorem of [19]. So by the Coates-Wiles theorem, we know that $E^{(d)}(p)(H) = E^{(d)}(p)[2]$, and the assertions follows immediately from Theorem 2.22. \square

Lemma 2.24. (i) If $q \equiv 3 \pmod{4}$ and splits in K , $q = f \cdot \bar{f}$ with f as in Lemma 2.15, then $(\frac{f}{\pi})(\frac{\pi}{\bar{f}}) = 1$, $(\frac{\bar{f}}{\pi})(\frac{\pi}{f}) = -1$ and $(\frac{f}{\pi}) = (\frac{\bar{f}}{f})$;

(ii) If $q \equiv 1 \pmod{4}$ and splits in K , $q = f \cdot \bar{f}$ with f as in Lemma 2.15, then $(\frac{f}{\pi})(\frac{\pi}{\bar{f}}) = 1$, $(\frac{\bar{f}}{\pi})(\frac{\pi}{f}) = 1$ and $(\frac{f}{\pi}) = (\frac{\bar{f}}{f})$.

Proof. (i) Write $f = a + b\frac{1+\pi}{2}$, then $a \equiv 1 \pmod{4}$ and $v_2(b) = 1$ as in Lemma 2.15.

By [?], P415, Theorem(8.3), we have $(\frac{f}{\pi})(\frac{\pi}{\bar{f}}) = (\frac{f\pi}{\omega})(\frac{f\pi}{\bar{\omega}})$. But as $f \equiv 1 \pmod{\omega^2}$ and $\pi = 1 - 2\frac{1-\pi}{2} \equiv 1 \pmod{\bar{\omega}^2}$, by [?], Chapter3, Theorem1, we deduce that $(\frac{f\pi}{\omega}) = (\frac{f\pi}{\bar{\omega}}) = 1$, hence $(\frac{f}{\pi})(\frac{\pi}{\bar{f}}) = 1$.

Because both \bar{f} and π are congruent to -1 modulo ω^2 , and $\pi \equiv 1 \pmod{\bar{\omega}^2}$, we have $(\frac{\bar{f}\pi}{\omega}) = -1$ and $(\frac{\bar{f}\pi}{\bar{\omega}}) = 1$, hence $(\frac{\bar{f}}{\pi})(\frac{\pi}{f}) = -1$.

Now we show $(\frac{f}{\pi}) = (\frac{\bar{f}}{f})$. As $(\frac{f}{\pi})(\frac{\pi}{\bar{f}}) = 1$, we only need to show that $(\frac{\pi\bar{f}}{f}) = (\frac{-b}{q}) = 1$. Since $v_2(b) = 1$, we have $(\frac{-b}{q}) = (\frac{2}{q})(\frac{-b/2}{q}) = (\frac{2}{q})(\frac{q}{(-b/2)})(\frac{2}{q})$.

Because $a^2 + ab + b^2\frac{p+1}{4} = q^h$ and h is odd, we have $(\frac{q}{(-b/2)}) = 1$.

Because $2 \mid b$, we have $a^2 + ab \equiv 1 + ab \equiv q^h \pmod{8}$. Then if $q \equiv 3 \pmod{8}$, we have $b \equiv 2 \pmod{8}$; if $q \equiv 7 \pmod{8}$, we have $b \equiv 6 \pmod{8}$, so that $(\frac{2}{q})(\frac{2}{q}) = 1$ always holds. This finishes the proof of (i).

(ii) The proof of the first two assertions are similar to the proof in (i), and we show $(\frac{f}{\pi}) = (\frac{\bar{f}}{f})$, or equivalently, $(\frac{-b}{q}) = 1$.

Assume $|-b| = 2^e c$ with c odd, then $(\frac{-b}{q}) = (\frac{2}{q})^e (\frac{c}{q})$.

Because $a^2 + ab + b^2\frac{p+1}{4} = q^h$ and h is odd, we have $(\frac{q}{c}) = 1$.

If $q \equiv 1 \pmod{8}$, then $(\frac{-b}{q}) = (\frac{2}{q})^e = 1$. If $q \equiv 5 \pmod{8}$, then $1 + ab \equiv 5 \pmod{8}$, hence $b \equiv 4 \pmod{8}$, i.e. $e = 2$. So we also have $(\frac{-b}{q}) = 1$. \square

Proposition 2.25. If $q \equiv 3 \pmod{4}$ splits in K , then

$$\text{rank}_{\mathcal{O}/2\mathcal{O}} S^{(q^*)} = 3$$

Proof. Notations as above.

If $(\frac{f}{\pi}) = 1$, then it's easy to verify by the above Lemma and Theorem 2.18 that $(f, 1)$ and $(1, \bar{f})$ generate $S^{(q^*)}$. On the other hand, if $(\frac{f}{\pi}) = -1$, then it is generated by $(-\bar{f}, 1)$ and $(1, -f)$. \square

Proposition 2.26. Suppose $d = \prod_{j=1}^m q'_j$ with $q'_j \equiv 1 \pmod{4}$ split in K , and g_j as in Lemma 2.15. If $(\frac{g_i}{\pi}) = -1$ for any j and $(\frac{g_k}{g_j}) = (\frac{g_k}{g_j}) = -1$, then

$$E^{(d)}(p)(H) = E^{(d)}(p)[2] \text{ and } (\text{III}(E^{(d)}(p)/H)[2])^{\text{Gal}(H/K)} = 1$$

Proof. As $g_j - 1 \equiv 1 \pmod{4}$ and hence $\bar{g}_j - 1 \equiv 1 \pmod{4}$, we have $(\frac{x}{y}) = (\frac{y}{x})$ for any $x, y \in G$, i.e. G is an unoriented grapha. The hypothesis implies that there is an arrow between any two vertexes of G , and since there are odd number of vertexes, we know G is an odd graph. \square

3. HEEGNER POINTS ON EISENSTEIN QUOTIENTS

3.1. Eisenstein quotients. In this section, let $X = X_0(N)/\mathbb{Q}$ be the modular curve of level some positive integer N , $J = J_0(N)/\mathbb{Q}$ be its Jacobian and $\mathbb{T} = \mathbb{Z}[\{T_\ell\}_\ell] \subseteq \text{End}(J/\mathbb{Q})$ be the (full) Hecke algebra of level N .

Recall that as Riemann surfaces, we have $X(\mathbb{C}) = \Gamma_0(N) \backslash \mathfrak{H}^*$, where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ and \mathfrak{H} is the upper-half plane. The points of $S = \Gamma_0(N) \backslash \mathbb{P}^1(\mathbb{Q})$ are called cusps of X and are known to be rational over $\mathbb{Q}(\mu_N)$. Take $i : X \rightarrow J$ to be the natural morphism which sending x to $[x] = (x) - (\infty)$. This morphism is defined over \mathbb{Q} because (∞) is \mathbb{Q} -rational, hence i induces a homomorphism of $G_{\mathbb{Q}}$ -modules (also denoted by i) $i : \text{Div}^0(X) \rightarrow J(\bar{\mathbb{Q}})$. We define the *cuspidal subgroup* of J to be the image of $\text{Div}^0(S)$ under i and denote it by C . Then C has a structure of $\mathbb{T}[G_{\mathbb{Q}}]$ -module because the action of \mathbb{T}

preserves cusps. More over, as we know that C is a finite group, we can also view C as a finite group scheme of J .

Definition 3.1. Suppose $P \in C$ is Hecke-eigen, that is to say the subgroup $\mathbb{Z} \cdot P$ of C is stable under \mathbb{T} . Then we define $\mathbb{I}(P)$ to be the ideal of \mathbb{T} annihilates P and we shall call it the Eisenstein ideal corresponding to P . So if P is of order n , then we have an isomorphism $\mathbb{T}/\mathbb{I}(P) \simeq \mathbb{Z}/n\mathbb{Z}$ and we define $m_q = (q, \mathbb{I}(P))$ for any prime divisor q of n .

For any $q \mid n$, let $m_q = (q, \mathbb{I})$. Define the Eisenstein quotient corresponding to P to be

$$\tilde{J}(P) = J / \left(\bigcap_{k \geq 0} \mathbb{I}^k \right) J$$

and the q -Eisenstein quotient corresponding to P to be

$$\tilde{J}^{(q)}(P) = J / \left(\bigcap_{k \geq 0} m_q^k \right) J$$

for any $q \mid n$.

Now assume K to be an imaginary quadratic field in which all the prime divisor of N splits (i.e. (K, N) satisfies the Heegner hypothesis). Then for any integer c prime to N , there exists an ideal \mathfrak{N}_c in \mathcal{O}_c such that $\mathcal{O}_c/\mathfrak{N}_c \cong \mathbb{Z}/N\mathbb{Z}$. Let

$$x_c = \mathbb{C}/\mathcal{O}_c \rightarrow \mathbb{C}/\mathfrak{N}_c^{-1} \in X(H_c)$$

where H_c is the ray class field of K . Hence we construct a point $[x_c]$ in $J(H_c)$. For any character $\chi : \text{Gal}(H_c/K) \rightarrow \mathbb{C}^\times$, define

$$y_\chi = \sum_{\sigma \in \text{Gal}(H_c/K)} \chi^{-1}(\sigma) [x_c^\sigma]$$

in $J(H_c) \otimes \mathbb{C}^\times$. When $c = 1$ and χ is trivial, we denote the corresponding point by y_K . The finite dimensional vector space $J(H_c) \otimes \mathbb{C}$ also admit a natural action by \mathbb{T} , which commutes with the action of G_Q . For any homomorphism of algebras $f : \mathbb{T} \rightarrow \mathbb{C}$, define $y_{\chi, f}$ to be the projection of y_χ on $(J(H_c) \otimes \mathbb{C})^{\chi, f}$. The basic question is to determine whether these point $y_{\chi, f}$ is zero.

In the following subsection, we introduce a method (due to Gross) to test whether the projection of the Heegner points on the Eisenstein quotients are non-torsion.

3.2. Eisenstein descent. The canonical morphism i induces an isomorphism $i^* : \hat{J} \simeq J$. Let P be a cuspidal point of order n defined over some field $M(\subseteq \mathbb{Q}(\mu_N))$, and D a cuspidal divisor representing P . Let P' be the inverse image of P under i^* .

Then P' gives a morphism of G_M -modules $J[n] \rightarrow \mu_n$ via the Weil pairings. Combining this with the Kummer map $J(F)/nJ(F) \rightarrow H^1(F, J[n])$ where F is some number field containing M , we get a map of G_F -modules

$$\delta(P) : J(F)/nJ(F) \rightarrow F^\times \otimes \mathbb{Z}/n\mathbb{Z}$$

We call this the Eisenstein descent corresponding to P over F .

Proposition 3.2. $\delta(P)(\sum n_i(x_i)) = \prod f^{n_i}(x_i)$, where f is the modular unit such that $\text{div}(f) = nD$.

Proof. Let D' be the divisor on J representing P' . Then both nD' and $[n]^*D'$ are principle, say $nD' = \text{div}(F)$ and $[n]^*D' = \text{div}(G)$. By [11], P184, Lemma, $\langle Q, P' \rangle = G(x)/G(x+Q)$ for any $Q \in J[n]$. \square

Proposition 3.3. If P is \mathbb{T} -eigen and $T_\ell P = T_\ell^* P$ for any $\ell \mid N$, then $\delta(P)$ is a morphism of \mathbb{T} -modules.

Proof. Let $\alpha_\ell, \beta_\ell : X_0(\ell p^2) \rightarrow X$ be the two morphisms sending (E, C, D) (C the ℓ -part and D the p^2 -part) to (E, D) and $(E/C, (C+D)/D)$ respectively, then T_ℓ is by definition $\circ \beta_{\ell,*} \alpha_\ell^*$.

By the construction, $f(T_\ell z) = f(\ell z) \prod_{i=0}^{\ell-1} f(\frac{z+i}{\ell}) = \alpha_{\ell,*} \circ \beta_\ell^*(f)$. As $\text{div}(\alpha_{\ell,*} \circ \beta_\ell^*(f)) = \alpha_{\ell,*} \circ \beta_\ell^*[\text{div}(f)] = T_\ell^*[\text{div}(f)] = (\ell+1) \cdot \text{div}(f)$, so we are done. \square

When $\delta(P)$ is a homomorphism of \mathbb{T} -modules, we can further localize it and define

$$\delta(P)_q : J(F)/nJ(F) \bigotimes_{\mathbb{T}_{m_q}} \rightarrow F^\times \otimes \mathbb{Z}_q/n\mathbb{Z}_q$$

for any $q \mid n$

3.3. η -quotient. In this subsection, we will consider the Eisenstein descent in the case that P is given by a rational cuspidal divisor.

Let $\eta(z)$ be the Dedkind η -function and let $\eta_d(z) := \eta(dz)$ for any integer d . Let N be a positive integer as before. For any family of integers $r = (r_d)$ indexed by the positive divisors of N , define

$$g_r = \prod_{d|N} \eta_d^{r_d}$$

we call any such function a Dedkind η -product. We have the following proposition

Proposition 3.4. $g_r \in \mathbb{Q}(X)$ if and only if the following four conditions are satisfied:

- (1) $\sum_{d|N} r_d = 0$;
- (2) $\sum_{d|N} d r_d \equiv 0 \pmod{24}$;
- (3) $\sum_{d|N} \frac{N}{d} r_d \equiv 0 \pmod{24}$;
- (4) $\prod_{d|N} d^{r_d} \in \mathbb{Q}^{\times 2}$

Proof. See [9]. □

As representatives of the cusps of X , we choose $\frac{x}{d}$ where d is a positive divisor of N and $(x, d) = 1$ with x taken modulo $(d, \frac{N}{d})$. We call such a cusp is of level d and it is defined over $\mathbb{Q}(\mu_m)$ where $m = (d, \frac{N}{d})$. The cusps of level d form an orbit under the action of $\text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Let D_d be the rational divisor on X defined as the sum of the cusps of level d (each with multiplicity one) and P_d the corresponding rational point on J , that is to say $P_d \in C(\mathbb{Q})$. We have the following proposition for the relation between the rational cuspidal divisor on X and the Dedkind η -product.

Proposition 3.5. Let $D = \sum_{d|N} m_d \cdot D_d$ be a rational cuspidal divisor of degree 0 on X and P the corresponding point in $J(\mathbb{Q})$, then there is a Dedkind η -product $g_r \in \mathbb{Q}(X)$ such that $nD = \text{div}(g_r)$ where n is the order of P .

Proof. See [9]. □

Let K be an imaginary quadratic field in which all the prime divisor of N splits, then there is an ideal \mathfrak{N} in K such that $\mathcal{O}_K/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Let $y_K \in J(H_K)$ be the Heegner point. For each $d | N$, we denote by \mathfrak{N}_d the unique ideal such that $\mathfrak{N}_d | \mathfrak{N}$ and $\mathcal{O}_K/\mathfrak{N}_d \simeq \mathbb{Z}/d\mathbb{Z}$. For any Dedkind η -product $g_r \in \mathbb{Q}(X)$ for some $r = (r_d)_{d|N}$, we have

$$\prod_{d|N} \mathfrak{N}_d^{r_d} = \mathfrak{a}_r^{-2}$$

by the condition (4) of Proposition 3.4, for some rational ideal \mathfrak{a}_r in K .

Theorem 3.6. Let $D = \sum_{d|N} m_d \cdot D_d$ be a rational cuspidal divisor of degree 0 on X and P the corresponding point in $J(\mathbb{Q})$, $g_r \in \mathbb{Q}(X)$ is the Dedkind η -product such that $nD = \text{div}(g_r)$ where n is the order of P , then

$$\delta(P)(y_K - \overline{y_K}) \equiv \zeta \cdot \alpha_r^{h_r} \pmod{K^{\times n}}$$

where ζ is a root of unit in K , α_r is a generator of the ideal $\frac{\mathfrak{a}_r}{\alpha_r}^{o(\alpha_r)}$ as above and $h_r = \frac{h_K}{o(\alpha_r)}$.

In particular, suppose $\delta(P)$ is a homomorphism of \mathbb{T} -modules, q a prime divisor of n with $(q, 6) = 1$ and $\alpha_r^{h_r}$ is not zero in $K^\times \otimes \mathbb{Z}_q/n\mathbb{Z}_q$ and $J[m_q](K)^- = 0$, then the projection of y_K on the q -Eisenstein quotient corresponding to P is non-torsion.

Proof. From the definition of the Dedkind η -quotient and the condition (1) of Proposition 3.4, we have

$$g_r(y_K - \overline{y_K})^{24} = \prod_{\mathfrak{a}} \prod_d \frac{\Delta(\mathfrak{N}_d \mathfrak{a})^{r_d}}{\Delta(\mathfrak{a})} \cdot \frac{\Delta(\overline{\mathfrak{N}_d \mathfrak{a}})^{r_d}}{\Delta(\overline{\mathfrak{a}})}$$

We know that $\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{N}_d \mathfrak{a})}$ is an integral number in H_K which generates the ideal \mathfrak{N}_d^{12} , hence prove the first claim.

For the second claim, as q is prime to 6, we can ignore the root of unit above. Then $\delta(P)_q(y_K - \overline{y_K})$ is not zero, and so $y_K - \overline{y_K}$ is not zero in $J(K)^- \otimes \mathbb{T}_{m_q}$. Hence $\delta(P)_q(y_K - \overline{y_K})$ is either non-torsion or m_q -torsion. But we assume that $J(K)^-[m_q] = 0$, so we get the conclusion. □

4. PRIME LEVEL CASE

In this section, we let N to be a prime p .

4.1. Eisenstein quotients. Recall that the cusps of X are $[0]$ and $[\infty]$ which are all rational, so C is a cyclic group generated by $[0] - [\infty]$. In particular, it must be Hecke-eigen.

Let $\mathbb{T} = \mathbb{Z}[\{T_\ell\}_\ell] \subseteq \text{End}(J_0(p))$ be the Hecke algebra of level p , here ℓ runs through all rational primes. Note that by the theorem of Atkin-Lehner, we have $w_p = -T_p$ in this prime level case, so our \mathbb{T} is just the one used in [12]. Let $\mathbb{I} = (T_p - 1, \{T_\ell - (1 + \ell)\}_{\ell \neq p}) = (w_p + 1, \{T_\ell - (1 + \ell)\}_{\ell \neq p})$ be an ideal in \mathbb{T} , then \mathbb{I} annihilates C and we call \mathbb{I} the *Eisenstein ideal of level p* .

Proposition 4.1. *Notations as above and let $n = \frac{p-1}{(12, p-1)}$, then:*

- (1) *The order of C is n and $C = J(\mathbb{Q})_{\text{tor}}$;*
- (2) *\mathbb{T} acts transitively on C with kernel \mathbb{I} ;*
- (3) *Under the natural morphism $J \rightarrow \tilde{J}$, we have $C \simeq \tilde{J}(\mathbb{Q})_{\text{tor}}$.*

Proof. See [12], Theorem 1.2 of Chapter 3 and Theorem 9.7 of Chapter 2. □

So we have the Eisenstein quotient \tilde{J} , and the $\tilde{J}^{(q)}$ for each $q \mid n$

Let $f = (\frac{\Delta(z)}{\Delta(pz)})^{\frac{1}{m}}$ with $m = (p-1, 12)$, then $\text{div}(f) = n((0) - (\infty))$. For any number field F , define

$$\delta_F : D'_0(F) \rightarrow F^\times$$

by the formula

$$\delta_F(\sum a_i(x_i)) = \prod f(x_i)^{a_i}$$

where $D'_0(F)$ is the group of divisors of degree zero over F .

On principle divisors we find $\delta(\text{div}(g)) = g(\text{div}(f)) = (g(0)/g(\infty))^n$ by reciprocity. Hence δ induces a homomorphism

$$\delta_F : J(F) \rightarrow F^\times \otimes \mathbb{Z}/n\mathbb{Z}$$

This map is called the Eisenstein descent (corresponding to C) over F .

Here is an explanation why call this a descent. Consider the Kummer map $J(F)/nJ(F) \rightarrow H^1(F, J[n])$. By the Weil pairing, the cuspidal point $[0]$ in J of order n gives a homomorphism of $G_{\mathbb{Q}}$ -modules $J[n] \rightarrow \mu_n$. Then the composition of these two maps is just the δ_F given above.

Viewing $\mathbb{Z}/n\mathbb{Z}$ as \mathbb{T} -module by Proposition 4.1, it is easy to check that δ is a homomorphism of \mathbb{T} -modules. Then we have

$$\delta_{F,q} : J(F) \otimes \mathbb{T}_{m_q} \rightarrow \mathbb{Z}_q/n\mathbb{Z}_q$$

for any $q \mid n$.

4.2. Heegner points on $\tilde{J}^{(q)}$ for odd q . In this section, we summarize Gross' results.

Proposition 4.2. *Suppose $q \mid n$ and $(q, 6) = 1$. Let K to be an imaginary quadratic field in which p splits. If $v_p(h_K) < v_p(\frac{p-1}{(12, p-1)})$, then $y_K^{(q)}$ is of infinite order in $\tilde{J}^{(q)}(K)$ for odd q such that $(q, w_K) = 1$, where $y_K^{(q)}$ to be the projection of y_K to $\tilde{J}^{(q)}$.*

Proof. First we show that $\delta_K(y_K - \bar{y}_K) \neq 0$.

By definition, we have

$$\delta_{K,q}(y_K - \bar{y}_K) = \left(\prod_{\mathfrak{a} \in Cl(\mathcal{O}_K)} \frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{p}\mathfrak{a})} \frac{\Delta(\overline{\mathfrak{p}\mathfrak{a}})}{\Delta(\overline{\mathfrak{a}})} \right)^{\frac{1}{m}}$$

where \mathfrak{p} is a prime ideal in K over p . As for any ideal $\mathfrak{b} \in Cl(\mathcal{O}_K)$, $\frac{\Delta(\mathfrak{p}\mathfrak{a})}{\Delta(\mathfrak{a})}$ is a number in H_K generates \mathfrak{p}^{-12} , we find that

$$\delta_{K,q}(y_K - \bar{y}_K) = u \cdot \alpha^{\frac{12h}{m}} \pmod{K}^{\times n}$$

with $u \in \mathcal{O}_K^\times$ and $\alpha \in K^\times$ such that $(\alpha) = (\mathfrak{p}/\bar{\mathfrak{p}})^{o(\mathfrak{p})}$.

Note that α is not a q -th power in K . This is because if $x^q = \alpha$, then $(x) = (\mathfrak{p}/\bar{\mathfrak{p}})^{o(\mathfrak{p})/q}$. As $\bar{\mathfrak{p}}$ is the converse of \mathfrak{p} in the ideal class group, we find that $o(\mathfrak{p}) \mid \frac{2o(\mathfrak{p})}{q}$, which is impossible as q is odd.

So when $\text{ord}_q(h) < \text{ord}_q(n)$, we will have $\delta_{K,q}(y_K - \bar{y}_K) \neq 0$, hence $y_K \neq 0$ in $J(K)^- \otimes \mathbb{T}_{m_q}$.

Mazur shows that $J[m_q] = \mathbb{Z}/q\mathbb{Z} \oplus \mu_q$, so that $J(K)^-[m_q] = 0$, so all points in $J(K)^- \otimes \mathbb{T}_{m_q}$ is not torsion. This completes the proof. □

4.3. Heegner points on $\tilde{J}^{(2)}$.

Example 1. Suppose p is of the form $u^2 + 64$ for some (odd) integer u . Note that $2 \mid n$ in this situation, so that the 2-Eisenstein quotient $\tilde{J}^{(2)}$ exists.

On the other hand, it is known that when p is of the above form, there is a unique isogeny class of elliptic curves of conductor p such that each curve in it has a point of order 2 ([14]). These curves are called Neumann-Setzer curves.

If E is a Neumann-Setzer curve, then E is a factor of $\tilde{J}^{(2)}$ ([12], Chapter3, Proposition7.4). Moreover, if $u = \pm 3 \pmod{8}$, then $\tilde{J}^{(2)}$ is simple ([12], Chapter3, Proposition7.5), so is a Neumann-Setzer itself.

We recall the following lemma

Lemma 4.3. (*Birch's Lemma*) *Let A be an abelian variety over \mathbb{Q} and $f : X_0(N) \rightarrow A$ be a morphism over \mathbb{Q} . If $f + f^{w_N}$ is a constant which does not belong to $2 \cdot A(\mathbb{Q})$, then the image of the Heegner point y_K on A is not torsion, here w_N is the Atkin-Lehner involution.*

Proof. *** □

For the 2-Eisenstein quotient, we can prove the following

Theorem 4.4. *Suppose $2 \mid \frac{p-1}{(12, p-1)}$. If h_K is odd, then $y_K^{(2)}$ is of infinite order in $\tilde{J}^{(2)}(K)$.*

Proof. Consider the morphism $f : X \rightarrow \tilde{J}^{(2)}$ obtained from the composition of the natural $X \rightarrow J$ and the projection $J \rightarrow \tilde{J}^{(2)}$.

By the definition of the Eisenstein ideal \mathbb{I} , we know that w_p acts as -1 on \tilde{J} and hence also -1 on $\tilde{J}^{(2)}$, so $f + f^{w_p}$ is a constant morphism. The image is just the projection of $[0] - [\infty]$.

By Theorem ??, the projection of $[0] - [\infty]$ on $\tilde{J}^{(2)}$ is a generator of $\tilde{J}^{(2)}(\mathbb{Q})$ which is a cyclic 2-group. In particular, the image of $f + f^{w_p}$ is not in $2 \cdot \tilde{J}^{(2)}(\mathbb{Q})$, so we get the conclusion by using Birch's Lemma. □

Corollary 4.5. *Suppose p is of the form $u^2 + 64$ with $u = \pm 3 \pmod{8}$ and let E be a Neumann-Setzer curve. If K is an imaginary quadratic field with odd class number such that p splits in K , then $\text{rank}_{\mathbb{Z}}(E(K)) = 1$ and $\text{III}(E/K)$ is finite.*

Remark 4.6. When p is inertia in K , we have the following results of Mazur and Gross (See [13], Page231 and [4]):

(1) Suppose q is an odd divisor of $\frac{p-1}{(12, p-1)}$ and $(q, K) \neq (3, \mathbb{Q}(\sqrt{-3}))$. If K is an imaginary quadratic field such that p is inertia in K and $q \nmid h_K$ where h_K is the class number of K , then $\tilde{J}^{(q)}(K)$ is finite and $\text{III}(J/K)[m_q] = 0$;

(2) Assume $2 \mid \frac{p-1}{(12, p-1)}$. If K is an imaginary quadratic field such that p is inertia in K and h_K is odd, then there is a cusp form which is congruent to $\delta \pmod{2}$, such that $L(f, K, 1) \neq 0$, where δ is the Eisenstein series.

So if p is of the form $u^2 + 64$ with $u = \pm 3 \pmod{8}$ and K is an imaginary quadratic field such that p is inertia in K and h_K is odd, then $E(K)$ is finite for any Neumann-Setzer curve E , because there is a non-trivial morphism $E \rightarrow \tilde{J}^{(2)}$ and $\tilde{J}^{(2)}$ is simple when $u = \pm 3 \pmod{8}$ as we mentioned in Example 1.

5. LEVEL p^2 CASE

In this section, we let $N = p^2$ be the square of a prime p .

5.1. Eisenstein quotients. Let p be prime and X/\mathbb{Q} the modular curve of level p^2 .

The cusps of X are $[0]$, $[\infty]$ and $\{\frac{i}{p}\}_{1 \leq i \leq p-1}$ with $[0]$ and $[\infty]$ \mathbb{Q} -rational and $\{\frac{i}{p}\}_{1 \leq i \leq p-1}$ form one orbit of $G_{\mathbb{Q}}$. So the rational cuspidal divisor subgroup of $J(\mathbb{Q})$ C is generated by $C_1 = [0] - [\infty]$ and $C_p = \sum_{i=1}^{p-1} [\frac{i}{p}] - (p-1)[\infty]$. We know that both C_1 and C_p have order $n = \frac{p^2-1}{24}$, and $C \cong (\mathbb{Z}/\frac{p-1}{(p-1, 12)}\mathbb{Z})^{\oplus 2} \oplus (\mathbb{Z}/\frac{p+1}{(p+1, 12)}\mathbb{Z})$ (see [7]).

Let $\mathbb{T} = \mathbb{Z}[\{T_n\}] \subseteq \text{End}(J/\mathbb{Q})$ be the ring of Hecke algebra of level p^2 .

From the definition of the Hecke actions, we have $T_p \cdot C_p = 0$ and $(T_l - (1+l)) \cdot C_p = 0$ for any $l \neq p$. Let

$$\mathbb{I} = (T_p, \{T_l - (1+l)\}_{l \neq p})$$

be an ideal in \mathbb{T} , which will be called the *Eisenstein ideal of level p^2 corresponding to C_p* .

By the above Lemma, we see that there is a surjective homomorphism $\mathbb{T}/\mathbb{I} \rightarrow \mathbb{Z}/n\mathbb{Z}$ given by the action of \mathbb{T} on C_p .

Lemma 5.1. *There is an integer m such that $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{T}/\mathbb{I}$.*

Proof. It is clear that the natural $\mathbb{Z} \rightarrow \mathbb{T}/\mathbb{I}$ is surjective.

If $\mathbb{Z} \cong \mathbb{T}/\mathbb{I}$, then under the perfect pairing

$$\mathbb{T} \times S_2(\Gamma_0(p^2), \mathbb{Z}) \rightarrow \mathbb{Z}$$

([15] for the notations and results), we find that $S_2(\Gamma_0(p^2), \mathbb{Z})[\mathbb{I}] \cong \mathbb{Z}$ which means there is a rational newform whose eigenvalues a_l is $l + 1$ for any $l \neq p$. But this will give an elliptic curve over \mathbb{Q} which is supersingular at all good places, which is impossible.

So there is an $m \in \mathbb{Z}$ such that $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{T}/\mathbb{I}$. \square

Let $\delta(z) = \sum_{(m,p)=1} \sigma(m)q^m$ ($q = e^{2\pi iz}$).

Lemma 5.2. $\delta(z) \in M_2(\Gamma_0(p^2), \mathbb{Z})[\mathbb{I}]$.

Proof. Let $e(z) = (1-p) - 24 \sum_{m=1}^{\infty} \sigma'(m)q^m$ ($q = e^{2\pi iz}$) which is in $M_2(\Gamma_0(p), \mathbb{Z})$ ([12], our e is his e'), and $e^{(p)}(z) = e(pz)$. It is easy to see that $\delta = \frac{1}{24}(e^p - e)$, so it is in $M_2(\Gamma_0(p^2), \mathbb{Z})$. It is easy by definition that δ is annihilated by \mathbb{I} . \square

From ([12], Chapter2, section5) we know the expansion of e at 0 is

$$e|[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}]_2 = \frac{1}{p}(p-1) + 24 \sum \frac{\sigma'(m)}{p} q^{\frac{m}{p}}.$$

We can use this to determine the Fourier expansion of δ at $[0]$ and $[\frac{i}{p}](1 \leq i \leq p-1)$:

- At $[\frac{i}{p}]$: Take $u, v \in \mathbb{Z}$ such that $ui - pv = 1$, then we have

$$\delta|[\begin{pmatrix} i & v \\ p & u \end{pmatrix}]_2 = \frac{p^2-1}{24p} + \dots$$

- At $[0]$:

$$\delta|[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}]_2 = \frac{(p^2-1)(1-p)}{24p} + \dots$$

Lemma 5.3. *Let d be an integer prime to p , if $\delta \in S_2(\Gamma_0(p^2), \mathbb{Z}/d\mathbb{Z})$, then $d|n$.*

Proof. By definition, $\delta \in S_2(\Gamma_0(p^2), \mathbb{Z}/d\mathbb{Z})$ if and only if there are $f \in S_2(\Gamma_0(p^2), \mathbb{Z})$ and $g \in M_2(\Gamma_0(p^2), \mathbb{Z})$ such that $\delta = f + dg$.

Since $g \in M_2(\Gamma_0(p^2), \mathbb{Z})$, we know the expansion of g at any cusps belong to $\mathbb{Z}[\frac{1}{p}, \zeta_{p^2}]$ by ([6], Chapter1, Cor1.6.2). The assertion follows from this and the discussion of the expansions of δ above. \square

Theorem 5.4. $(\mathbb{T}/\mathbb{I}) \otimes \mathbb{Z}[\frac{1}{p}] \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. Let m be as in Lemma 5.1.

From the perfect pairing

$$\mathbb{T} \times S_2(\Gamma_0(p^2), \mathbb{Z}) \rightarrow \mathbb{Z}$$

we get a perfect pairing

$$\mathbb{T}/m\mathbb{T} \times S_2(\Gamma_0(p^2), \mathbb{Z}/m\mathbb{Z}) \rightarrow \mathbb{Z}/m\mathbb{Z}$$

Then we have

$$\mathbb{T}/\mathbb{I} \times S_2(\Gamma_0(p^2), \mathbb{Z}/m\mathbb{Z})[\mathbb{I}] \rightarrow \mathbb{Z}/m\mathbb{Z}$$

or equivalently

$$\mathbb{T}/\mathbb{I} \cong \text{Hom}(S_2(\Gamma_0(p^2), \mathbb{Z}/m\mathbb{Z})[\mathbb{I}], \mathbb{Z}/m\mathbb{Z})$$

and so

$$(\mathbb{T}/\mathbb{I}) \otimes \mathbb{Z}[\frac{1}{p}] \cong \text{Hom}(S_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}]/m\mathbb{Z}[\frac{1}{p}])[\mathbb{I}], \mathbb{Z}[\frac{1}{p}]/m\mathbb{Z}[\frac{1}{p}])$$

By the q -expansion principle (see [6]), $S_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}]/m\mathbb{Z}[\frac{1}{p}])$ is generated by $c\delta$ for some $c|m$. Then we will have $c\delta = f + mg$ with some $f \in S_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}])$ and $g \in M_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}])$, then we get $\frac{1}{c}f = \delta - \frac{m}{c}g$ also in $S_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}])$. So $\delta \in S_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}]/\frac{m}{c}\mathbb{Z}[\frac{1}{p}])$, and hence $\frac{m}{c}|n$ by Lemma 5.3. So we see $\frac{m}{n}|c$, and hence $\#(S_2(\Gamma_0(p^2), \mathbb{Z}[\frac{1}{p}]/m\mathbb{Z}[\frac{1}{p}])[\mathbb{I}]) \leq n$. This completes the proof. \square

As in the prime level case, let $m_q = (q, \mathbb{I})$ be a maximal ideal in \mathbb{T} for any $q|n$. Define the *Eisenstein quotient of level p^2 corresponding to C_p* to be

$$\tilde{J} = J / \left(\bigcap_{k \geq 0} \mathbb{I}^k \right) J$$

and the *q -Eisenstein quotient of level p^2 corresponding to C_p* to be

$$\tilde{J}^{(q)} = J / \left(\bigcap_{k \geq 0} m_q^k \right) J$$

for any $q | n$.

Different from the prime level situation, the Atkin-Lehner involution w_p is not equal to the Hecke operator T_p when the level is p^2 . So we further define

$$\tilde{J}_{\pm}^{(q)} = (\tilde{J}^{(q)})^{w_p \pm 1 = 0}$$

5.2. Structure of $J[m_q]$. Let $S = \text{Spec}(\mathbb{Z}[\frac{1}{p}])$ and G/S any finite flat commutative group scheme over S . By ([12], Chapter1, P45-46), we have a natural bijection between $\{\text{flat closed subgroup schemes } H/S \text{ of } G/S\}$ and $\{\text{sub-}G_{\mathbb{Q}} \text{ modules of } G(\bar{\mathbb{Q}})\}$.

An S -group scheme G/S of order a power of q (q a rational prime) is called admissible if it is a finite flat group scheme over S and has a filtration of flat closed subgroup schemes $0 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$ such that $G_i/G_{i-1} \cong (\mathbb{Z}/q\mathbb{Z})/S$ or μ_q/S . By the above remarks, this is equivalent to say that $G(\bar{\mathbb{Q}})$ has a filtration of sub-representations with factors isomorphic to $\mathbb{Z}/q\mathbb{Z}$ or $\mu_q(\bar{\mathbb{Q}})$.

Proposition 5.5. *For any $q|n$, we have $J[m_q]$ is admissible.*

Proof. The proof is the same as in [12]. □

Fix a prime $q|n$, then the rational point $C_p \in J(\mathbb{Q})[\mathbb{I}]$ gives a rational point of $J[m_q]$, hence we have the exact sequence

$$0 \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow J[m_q] \longrightarrow V \longrightarrow 0$$

for some V/S which is also admissible.

Lemma 5.6. *If q is odd, then $V \cong (\mu_q)^{\oplus d}$ for some $d \geq 1$.*

Proof. First, we show V is of multiplicative type, i.e. there's no embedding of $\mathbb{Z}/q\mathbb{Z}$ in V .

Suppose that there is an embedding $\mathbb{Z}/q\mathbb{Z} \rightarrow V$. Let G be the pull back of this constant group scheme. Then there is an embedding of $(\mathbb{Z}/q\mathbb{Z})^{\oplus 2}$ in $J[m_q]$. By reduction to \mathbb{F}_q , we get

$$\dim_{\mathbb{F}_q}(J/\mathbb{F}_q)[I](\bar{\mathbb{F}}_q) \geq 2$$

which is impossible by the q -expansion principle as there is an injection $(J/\mathbb{F}_q)[I](\bar{\mathbb{F}}_q) \rightarrow H^0(X/\mathbb{F}_q, \Omega)$. This show that V is of multiplicative type.

By Eichler-Shimura, for any $l \nmid pq$, the Frobenius at l acting on V has eigenvalue 1 or l . But as q is odd, Frob_l can not have eigenvalue 1 on μ_q . So all the eigenvalues are l . Then by ([12], Chapter1, Lemma3.5), we have $V \cong (\mu_q)^{\oplus d}$ for some d .

By ([12], Chapter2, Lemma7.7), we deduce that $\dim_{\mathbb{F}_q} J[m_q](\bar{\mathbb{Q}}) \geq 2$, so $d \geq 1$. □

Theorem 5.7. *If $(q, 6) = 1$, then there is a non-split exact sequence*

$$0 \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow J[m_q] \longrightarrow \mu_q \longrightarrow 0$$

which determines the structure of $J[m_q]$ as the unique (up to scale) non-trivial element in $\text{Ext}_S^1(\mu_q, \mathbb{Z}/q\mathbb{Z})$.

Proof. Suppose the d in $\tilde{\text{ref}}\text{multiplicative type}$ is strictly larger than 2, then we will have a group scheme G/S and an exact sequence

$$0 \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow G \longrightarrow (\mu_q)^{\oplus 2} \longrightarrow 0$$

Let $f_i : \mu_q \rightarrow (\mu_q)^{\oplus 2}$ ($i = 1, 2$) be the two embedding. The pull backs will give us two elements in $\text{Ext}_S^1(\mu_q, \mathbb{Z}/q\mathbb{Z})$. But by ([2], Proposition4.2.1), $\dim_{\mathbb{F}_q} \text{Ext}_S^1(\mu_q, \mathbb{Z}/q\mathbb{Z}) = 1$ (as $(q, 6) = 1$ and $p = \pm 1 \pmod{q}$). So some linear combination of f_1 and f_2 will gives a sub-group scheme H of $J[m_q]$ which is isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mu_q$. In particular, there is an embedding of μ_q in $J[m_q]$.

By [18], we should have this μ_q contained in \sum -the Shimura subgroup of J . But by [8], T_p acts on \sum as multiplication by p , which contradicts that $\mu_q \subseteq J[m_q]$ which is annihilated by T_p . \square

Remark: This theorem implies that the Galois representation given by the action of $G_{\mathbb{Q}}$ is a two dimensional mod q reducible Galois representation, which is not semisimple.

5.3. Gross curves and the 2-Eisenstein quotient. Recall that for p be a prime which is congruent to 3 modulo 4, there is a unique isogeny class of \mathbb{Q} -curves over H with CM by \mathcal{O} and the associated character ϕ .

Let $f_{\phi}(z) = \sum_{(\mathfrak{a}, p)=1} \phi(\mathfrak{a}) \cdot e^{2\pi i \cdot N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot z} = \sum_{n \geq 1} a_n q^n$ ($z \in \mathcal{H}, q = e^{2\pi i z}$). By Lemma 3 of [16], $f_{\phi}(z)$ is an eigenform in $S_2(\Gamma_0(p^2))$. Let T be the field generated by the image of ϕ . Then T is a CM field with $T^+ = \mathbb{Q}(\{a_n\})$. By theorem 7.14 and theorem 7.15 of [17], there is a sub-abelian variety $i : A \rightarrow J$ over \mathbb{Q} and an embedding $\theta : T^+ \rightarrow \text{End}_{\mathbb{Q}}(A)$, such that $T_n|_A = \theta(a_n)$ for any n , where T_n is the Hecke operator.

Proposition 5.8. *There is a Gross curve such that $\text{Res}_{F/\mathbb{Q}} E \cong A$, where $F = \mathbb{Q}(j(E))$.*

Proof. By Theorem 1 of [16], A is isogenous to $E' \oplus^h$ for some elliptic curve with CM by \mathcal{O} . Then we have also A isogenous to $(E'^{\sigma}) \oplus^h$ for any $\sigma \in \text{Gal}(H/\mathbb{Q})$. So E' is isogenous to E'^{σ} for any $\sigma \in \text{Gal}(H/\mathbb{Q})$, i.e. E' is a \mathbb{Q} -curve (note that $\overline{\mathbb{Q}}$ -isogeny is automatically H -isogeny).

It is clear that there is a \mathbb{Q} -morphism between $\prod_{\sigma} (E')^{\sigma}$ and A . Because $\prod_{\sigma} (E')^{\sigma}$ is simple over \mathbb{Q} , this morphism must be an isogeny. Then, modulo the kernel, we find an E such that $\text{Res}_{F/\mathbb{Q}} E = \prod_{\sigma} (E')^{\sigma} \cong A$.

As $L(E/F, s) = L(s, \chi_E) = L(s, A/\mathbb{Q}) = \prod_{\tau} L(s, f^{\tau}) = L(s, \chi)$ (up to finite Euler factors), we have $\chi_E = \chi$. \square

Proposition 5.9. *Notations as above. If $p \equiv 7 \pmod{8}$, then $A \hookrightarrow \tilde{J}_+^{(2)}$. In particular, there is a non-trivial morphism $E \rightarrow \tilde{J}_+^{(2)}$ for any Gross curve E .*

Proof. This is because $A(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ and the ϵ -factor of its L-function is 1, when $p \equiv 7 \pmod{8}$ (see [5]). \square

5.4. Heegner point on $\tilde{J}^{(q)}$ for odd q .

Lemma 5.10. *Let η be the Dedekind η -function and $f = \frac{\eta(pz)^{p+1}}{\eta(z)\eta(p^2z)^p}$. Then f is a rational function on X defined over \mathbb{Q} , and $\text{div}(f) = n(P_p - (p-1)[\infty])$.*

Proof. compute by η -quotient theory. \square

As in [3], for any field F , we can define a homomorphism

$$\delta_F : J(F) \rightarrow F^{\times} \otimes \mathbb{Z}/n\mathbb{Z}$$

which sending any $\sum a_i [x_i] \in \text{Div}^0(X)(F)$ disjoint from $P_p - (p-1)[\infty]$ to $\prod f(x_i)^{a_i}$.

Recall that the action of \mathbb{T} on C_p gives a homomorphism $\mathbb{T}/\mathbb{I} \rightarrow \mathbb{Z}/n\mathbb{Z}$. We will view $\mathbb{Z}/n\mathbb{Z}$ as a \mathbb{T} -module in this way.

Lemma 5.11. *For any field F , the map δ_F is a \mathbb{T} -module homomorphism.*

Proof. It is enough to check the generators T_l for primes l .

Suppose first that $l \neq p$. Let $\alpha_l, \beta_l : X_0(lp^2) \rightarrow X$ be the two morphisms sending (E, C, D) (C the l -part and D the p^2 -part) to (E, D) and $(E/C, (C+D)/D)$ respectively, then T_l is by definition $\alpha_{l,*} \circ \beta_l^*$.

By the construction, $f(T_l z) = f(lz) \prod_{i=0}^{l-1} f(\frac{z+i}{l}) = \alpha_{l,*} \circ \beta_l^*(f)$. As $\text{div}(\alpha_{l,*} \circ \beta_l^*(f)) = \alpha_{l,*} \circ \beta_l^*[\text{div}(f)] = T_l(\text{div}(f)) = (l+1) \cdot \text{div}(f)$, we have $f(T_l z) = f^{(l+1)}(z)$ up to constant. When take value on zero divisors, the effect of constants disappears, so we are done.

For T_p , recall that $\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n)$ ($q = e^{2\pi i z}$), so we have

$$\begin{aligned} f(T_p z) &= \prod_{k=0}^{p-1} f\left(\frac{z+k}{p}\right) \\ &= \prod_{k=0}^{p-1} \frac{\eta(z+k)^{p+1}}{\eta(\frac{z+k}{p}) \cdot \eta(pz + pk)^p} \end{aligned}$$

18

$$\approx \prod_{k=0}^{p-1} \frac{\eta(z)^{p+1}}{\eta(\frac{z+k}{p}) \cdot \eta(pz)^p}$$

(\approx means "equal up to constant")

$$= \left[\frac{\eta(z)}{\eta(pz)} \right]^{p^2-1} \cdot \frac{\eta^{p+1}}{\prod_{k=0}^{p-1} \eta(\frac{z+k}{p}) \cdot \eta(pz)}$$

But we have

$$\eta(z)^{p+1} = q^{\frac{1+p}{24}} \prod_{n=1}^{\infty} (1 - q^n)^{1+p}$$

$$\eta(pz) = q^{\frac{p}{24}} \prod_{n=1}^{\infty} (1 - q^{pn})$$

and

$$\prod_{k=0}^{p-1} \eta\left(\frac{z+k}{p}\right) \approx q^{\frac{1}{24}} \prod_{k=0}^{p-1} \prod_{n=1}^{\infty} (1 - q^{\frac{n}{p}} \zeta^{kn})$$

(ζ a primitive p -th root of unity)

$$= q^{\frac{1}{24}} \cdot \left[\prod_{p|n} (1 - q^{\frac{n}{p}})^p \right] \cdot \left[\prod_{p \nmid n} (1 - q^n) \right]$$

So

$$f(T_p z) \approx \left[\frac{\eta(z)}{\eta(pz)} \right]^{p^2-1}$$

which implies that

$$\delta_F \circ T_p = 0$$

□

By the Lemma just proved, we have, for any field, a \mathbb{T} -module homomorphism

$$\delta_F : J(F) \otimes \mathbb{T}/\mathbb{I} \rightarrow F^\times \otimes \mathbb{Z}/n\mathbb{Z}$$

and hence for any $q|n$

$$\delta_{F,q} : J(F) \otimes \mathbb{T}_{m_q}/\mathbb{I}\mathbb{T}_{m_q} \rightarrow F^\times \otimes \mathbb{Z}/q^{n_q}\mathbb{Z}$$

where \mathbb{T}_{m_q} is the completion of \mathbb{T} at m_q and $n_q = \text{ord}_q(n)$.

Now let K be an imaginary quadratic field such that $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K .

Let $x_K = (\mathbb{C}/\mathcal{O}_K \rightarrow \mathbb{C}/\mathfrak{p}^{-1}) \in X(H_K)$ and $y_K = \sum_{\sigma \in G(H_K/\mathbb{Q})} \epsilon(\sigma) \cdot x_K^\sigma \in J(K)^-$, where ϵ is the quadratic character corresponding to K . For any $q|n$, let $y_K^{(q)}$ be the projection of y_K in $J^{(q)}(K)^-$.

Theorem 5.12. *Suppose $(q, 6) = 1$ and $q|(p+1)$. Let $h = h_k/o(\mathfrak{p})$. Then if $\text{ord}_q(h) < \text{ord}_q(n)$, then $y_K^{(q)}$ is a non-torsion point in $J^{(q)}(K)^-$.*

Proof. By definition, we have

$$\delta_{K,q}(y_K) = \prod_{\mathfrak{a} \in \text{Cl}(\mathcal{O}_K)} \left[\frac{\Delta(\mathfrak{p}\mathfrak{a})^{p+1}}{\Delta(\mathfrak{a})\Delta(\mathfrak{p}^2\mathfrak{a})^p} \cdot \frac{\Delta(\bar{\mathfrak{a}})\Delta(\overline{\mathfrak{p}^2\mathfrak{a}})^p}{\Delta(\bar{\mathfrak{p}}\bar{\mathfrak{a}})^{p+1}} \right]^{\frac{1}{24}}$$

As $\frac{\Delta(\mathfrak{p}\mathfrak{a})^{p+1}}{\Delta(\mathfrak{a})\Delta(\mathfrak{p}^2\mathfrak{a})^p} = \left[\frac{\Delta(\mathfrak{p}\mathfrak{a})}{\Delta(\mathfrak{p}^2\mathfrak{a})} \right]^p \frac{\Delta(\mathfrak{p}\mathfrak{a})}{\Delta(\mathfrak{a})}$ and for any ideal $\mathfrak{b} \in \text{Cl}(\mathcal{O}_K)$, $\frac{\Delta(\mathfrak{p}\mathfrak{a})}{\Delta(\mathfrak{a})}$ is a number in H_K generates \mathfrak{p}^{-12} , we find that

$$\delta_{K,q}(y_K) = u \cdot \alpha^{\frac{p-1}{2}h} \pmod{(K)^\times}$$

with $u \in \mathcal{O}_K^\times$ and $\alpha \in K^\times$ such that $(\alpha) = (\mathfrak{p}/\bar{\mathfrak{p}})^{o(\mathfrak{p})}$.

Note that α is not a q -th power in K . This is because if $x^q = \alpha$, then $(x) = (\mathfrak{p}/\bar{\mathfrak{p}})^{o(\mathfrak{p})/q}$. As $\bar{\mathfrak{p}}$ is the converse of \mathfrak{p} in the ideal class group, we find that $o(\mathfrak{p}) \mid \frac{2o(\mathfrak{p})}{q}$, which is impossible as q is odd.

So when $\text{ord}_q(h) < \text{ord}_q(n)$, we will have $\delta(y_K) \neq 0$, hence $y_k \neq 0$ in $J(K)^- \otimes \mathbb{T}_{m_q}$.

But by restructure, one easily see that $J(K)^-[m_q] = 0$, so all points in $J(K)^- \otimes \mathbb{T}_{m_q}$ is not torsion. This completes the proof. \square

5.5. Heegner point on Gross curves when $p \equiv 7 \pmod{8}$. Let $i : A \hookrightarrow J$ be the sub-abelian variety as in section 3.3 and E the Gross curve as in Theorem 5.8. Let $\pi : J \rightarrow A$ be the dual of i , where we have identify the dual of A and J with themselves.

Let $R_i = mC_i$ be of exact order 2, for $i = 1, p$.

Lemma 5.13. $R_1 = R_2$.

Proof. By Theorem 1 of [7], the prime to p part of the \mathbb{Q} -rational cuspidal divisor subgroup is isomorphic to $(\mathbb{Z}/a\mathbb{Z})^2 \oplus (\mathbb{Z}/b\mathbb{Z})$, where $a = \frac{p-1}{(p-1, 24)}$ and $b = \frac{p+1}{(p+1, 24)}$. But as $p = 7 \pmod{8}$, a is odd. So the 2-part of the \mathbb{Q} -rational cuspidal divisor subgroup is cyclic, hence the result. \square

By Theorem 22.1.1 of [5], we know that $A(\mathbb{Q}) = \langle P \rangle \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Lemma 5.14. $R_1 \in J[m_2]$.

Proof. Only need to check this for T_p . But $T_p(R_1) = T_p(mC_1)m(C_1+C_p) = 0$ as $T_p = \sum_{0 \leq j \leq p-1} \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$, so the result follows from Lemma 5.13. \square

Proposition 5.15. $P \in J[m_2]$

Proof. By Shimura's theorems, we know that $T_p = 0$ on A as $a_p = 0$, and $(l+1)-T_l(P) = (l+1-\theta(a_l))(P)$ for $l \neq p$. To prove the theorem, it is sufficient to show $2 \mid \deg(l+1-\theta(a_l))$. By the construction of A , $\deg(l+1-\theta(a_l)) = |\det(l+1-\theta(a_l))|^2 = N_{T^+/\mathbb{Q}}(l+1-\theta(a_l))$. As $N_{T^+/\mathbb{Q}}(l+1-\theta(a_l)) = \#A \pmod{l}(\mathbb{F}_l)$, the result follows from Lemma 5.16. \square

Lemma 5.16. $A(\mathbb{Q})[2] \hookrightarrow A \pmod{l}(\mathbb{F}_l)$ for any $l \neq p$.

Proof. As A has good reduction at l when $l \neq p$, we know that $A(\mathbb{Q})[2] \hookrightarrow A \pmod{l}(\mathbb{F}_l)$ for any $l \nmid 2p$.

So we only need to show $A(\mathbb{Q})[2] \hookrightarrow A \pmod{2}(\mathbb{F}_2)$.

Consider the sub-abelian variety E of A over H as in Prop 5.8. Let w be a place of H over 2 and \mathfrak{p} the prime of K below w . Suppose $P \pmod{2} = 0$. Then in terms of E , we have $P \in \hat{E}$ where \hat{E} is the formal group at w . But \hat{E} is a lubin-Tate formal group, which implies that $P \in E[\mathfrak{p}^\infty]$. This contradicts that $P \in E(F)$ and $F = H^\tau$ where τ is the complex multiplication. \square

Theorem 5.17. Suppose $p = 7 \pmod{8}$, K an imaginary quadratic field in which p splits and y_K be the Heegner point. If $\tilde{J}^{(2)}$ is simple and the class number of K is odd, then the projection of y_K on A is not torsion.

Proof. When $p = 7 \pmod{8}$, the ϵ -factor is 1. So to apply Birch's Lemma, we only need to verify $\pi(C_1)$ is not in $2 \cdot A(\mathbb{Q})$.

Suppose $\pi([0] - [\infty]) \in 2 \cdot A(\mathbb{Q})$, then $\pi(C_1) = 0$ as we know that $A(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. Let $B = \ker(\pi)$, then we have $P \in B[m_2]$ by Proposition 5.15. So there is a newform $g \in S^{\text{new}}(\Gamma(p^2))$ such that $A_g \subseteq B$ and $A_g[m_2] \neq 0$, in particular this sub-abelian variety A_g will be contained in $\tilde{J}^{(2)}$.

But $A \not\subseteq B$ as the composition $\pi \circ i$ is multiplication by $\deg(\pi)$, so $A \neq A_g$ which contradicts our assumption that $\tilde{J}^{(2)}$ is simple. \square

REFERENCES

- [1] A.Brumer, K.Krammer, Paramodular abelian varieties of odd degree, Transactions of the American Mathematical Society, 2012, 366(5):769-77
- [2] A.Brumer and K.Kramer, The rank of elliptic curves, Duke Math.J.(4) 44, (1977), 715-743
- [3] B.Gross, Heegner point on $X_0(N)$, Modular forms (Durham), 1982
- [4] B.Gross, Heights and the special value of L-series, Number Theory, 1985, 27(10):115-187
- [5] B.Gross, Arithmetic of elliptic curves with complex multiplication, Lecture Notes in Mathematics, 1980, 776(1):327-337
- [6] N.Katz, P-adic properties of modular schemes and modular forms, Lecture Notes in Mathematics 350, pp 69-190
- [7] S.Ling, Rational cuspidal subgroup of $J_0(p^r)$, Israel Journal of Mathematics, 1997, 99(1):29-54
- [8] S.Ling, J.Osterele, Shimura subgroup of $J_0(N)$, Astrisque 196C197 (1991), 171C203.
- [9] G.Ligozat, Courbes modulaires de genre 1, Bull. Soc. Math. France Mem. 43(1975)
- [10] D.Mumford, J.Forgarty, Kirwan, Geometric invariant theory, Springer, 1965, 93(4):99-127
- [11] D.Mumford, Abelian variety, Tata Institute of Fundamental Research Studies in Mathematics, 1970, 27(7-8):338-354
- [12] B.Mazur, Eisenstein ideals and modular curves, Publications mathematiques de l'IHS, 1977, 47(1):33-186

- [13] B.Mazur, On the Arithmetic of Special Value of L Function, *Inventiones mathematicae*, 1979, 55(3):207-240
- [14] NS-curve
- [15] K.Ribet, Mod p Hecke operators and congruences between modular forms, *Inventiones mathematicae*, 1983, 71(1):193-205
- [16] G.Shimura, Elliptic curves with CM as factors of Jacobians of modular fuctions, *Nagoya Mathematical Journal*, 1971, 43:199-208
- [17] G.Shimura, Introduction to the arithmetic theory of automorphic functions, *Publications of the Mathematical Society of Japan*, 11
- [18] Vatsal, Multiplicative subgroup of $J_0(N)$, *Journal of the Institute of Mathematics of Jussieu*, 2005, 4(2):281-316
- [19] T.Yang, Nonvanishing of certain Hecke L-series and rank of certain elliptic curves, *compositio math.* 117 (1999), No.3, 337-359.